UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MASSACHUSETTS

LEONARD LICHT, ZHENGJUN CAI, HENRY CHEN, DANIEL CHANG, DOMINIC CHOW, CHENGGUO DONG, IHAB W. FRANCIS, JOHN GORDON, DALTON GREEN, MICHAEL GRILLI, IRAKLIS KARABASSIS, NADER LOBANDI, JAMES MOSKWA, ANH NGUYEN, BRIAN ROTHAUS, GORDON SHAYLOR, RICHARD SLAVANT, NATHANIAL THRAILKILL, JACK YAO, and JUN ZHAI,

Plaintiffs,

v.

BINANCE HOLDINGS LIMITED, d/b/a BINANCE.COM, BAM TRADING SERVICES, INC., d/b/a BINANCE.US, and CHANGPENG ZHAO,

Defendants.

No. 24-cv-10447

JURY DEMANDED ON ALL CAUSES OF ACTIONS

Leave to File Granted at ECF No. 78 (February 26, 2025)

SECOND AMENDED COMPLAINT

Lead plaintiff Leonard Licht and the 19 co-Plaintiffs identified herein bring this second amended complaint against Defendants Binance Holdings Limited ("Binance"), BAM Trading Services, Inc. ("BAM"), and Changpeng Zhao ("Zhao") pursuant to the federal civil Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1964(c).

I. INTRODUCTION

1. Binance is a Cayman Islands corporation that operates the world's largest cryptocurrency exchange, Binance.com. Binance was founded by Zhao. Zhao maintained

majority ownership of Binance and served as its CEO until November 2023, amassing a fortune that made him the 69th richest person in the world, according to Forbes Magazine. For years, however, Binance and Zhao knowingly and willfully operated the Binance.com exchange in flagrant violation of United States criminal statutes, including anti-money laundering statutes and statutes prohibiting unlicensed money transmitting businesses.

2. Binance profited handsomely from its crimes, but federal prosecutors eventually caught on to Binance's schemes. On November 21, 2023, Binance and Zhao pled guilty, in the United States District Court for the Western District of Washington, to several federal crimes, including (1) conspiracy to violate the anti-money laundering requirements of the federal Bank Secrecy Act, 31 U.S.C. §§ 5318(h) and 5322; and (2) conspiracy to conduct an unlicensed money transmitting business, 18 U.S.C. §§ 1960(a) and 1960(b)(1)(B). *See United States of America v. Binance Holdings Ltd., No. 23-cr-178, Dkt. #21*; *United States of America v. Changpeng Zhao, No. 23-cr-179*, Dkt. #29. Binance's plea agreement requires it to pay a criminal fine of more than $1.8 billion and criminal forfeiture of more than $2.5 billion, and on April 30, 2024, Zhao was sentenced to a term of imprisonment of four months and ordered to pay a criminal fine of $50 million as a consequence of his plea.

3. As Judge Jones explained at Zhao's sentencing, "I was deeply troubled . . . by [Zhao's] statement . . . that it was better to ask for forgiveness than permission." The Judge further described Zhao's and Binance's crimes as "unprecedented in terms of volume, scale and massiveness in dollar impact of noncompliance." Shockingly, and straining all credulity, Zhao's defense attorneys consistently referred to Zhao's conduct as a "mistake." But it was not a "mistake"—it was purposeful, intentional conduct over a multi-year period that was documented in thousands of contemporaneous business records showing that Binance's business model, as

orchestrated and directed by Zhao, was predicated on facilitating criminal activity around the globe, including the pig butchering schemes that ensnared the Plaintiffs. In any event, none of those fines or forfeiture, or even Zhao's request for "forgiveness," will provide solace, let alone compensation, to the flesh and blood victims of Binance's and Zhao's crimes, whose lives have been shattered as a direct result of the Defendants' actions.

4. Binance's and Zhao's crimes were not victimless regulatory infractions. To the contrary, Binance's and Zhao's systematic criminal conduct—conduct that defendant BAM also participated in and conspired with—enabled criminal syndicates to ensnare innocent, vulnerable victims into financially devastating cryptocurrency fraud schemes, including one type of predatory scheme known as "pig butchering." To successfully complete their frauds, these criminal syndicates, which stole crypto-assets from innocent victims, needed a high-liquidity, high-volume centralized cryptocurrency exchange to allow them to convert the stolen crypto into U.S. dollars or other forms of fiat currency. Binance and Zhao knowingly and willfully allowed the criminal syndicates to use the Binance.com exchange to do this—that is, to launder their illicitly obtained cryptocurrency and convert those otherwise traceable assets into untraceable, unrecoverable fiat currency—therefore aiding and abetting the syndicates' wire frauds and money laundering activities. BAM participated in and conspired with those racketeering acts as well. In short, Binance and Zhao, with BAM's participation and assistance, knowingly and willfully provided the pig butchering syndicates with the "getaway car" that was an indispensable component of their fraud schemes. Binance did so for a very simple reason: money. Binance received lucrative fees on every transaction that the criminal syndicates conducted on the Binance.com exchange, which amounted to hundreds of millions of dollars in illicit profits for Binance.

5. This complaint is brought by 20 innocent victims of Zhao's and Binance's crimes, 18 of whom are American citizens and all of whom have resided in the United States during all relevant times. The Plaintiffs are hardworking, ordinary people who lost significant sums of money—in some instances, life-changing sums of money—in fraudulent "pig butchering" schemes that (i) utilized and were accomplished through the Binance.com exchange; (ii) were facilitated and aided and abetted by the Defendants' knowing and willful conduct (namely, ensuring that fraud syndicates would be permitted to freely use the Binance.com exchange as the laundering facility and cash-out point that was a necessary component of the syndicates' wire fraud schemes); and (iii) could not have succeeded but for the Defendants' systematic, prolonged, and willful violations of federal criminal laws that Congress rightfully has declared to be RICO predicate acts. The money and cryptocurrency assets that were fraudulently stolen from the Plaintiffs was located in the United States at the time of the thefts, and the fraudsters knew they were stealing from U.S.-based victims.

6. One Plaintiff, Lenny Licht was bilked out of almost $3 million by a pig butchering syndicate. The fraud began when Lenny was contacted on Facebook—a social media site that conspicuously identified Lenny as residing in Plano, Texas—by an individual who claimed to be a common friend of one of Lenny's high school classmates. The individual then moved the conversation to WhatsApp, using Lenny's clearly U.S.-based phone number. The individual then convinced Lenny to purchase millions of dollars in cryptocurrency on the U.S.-based exchange Coinbase.com and then to transfer those assets to an electronic address that, unbeknownst to Lenny, was actually self-custodied (*i.e.*, off-exchange) digital wallet controlled by the fraudsters. Once Lenny realized that he had been defrauded, he sought to recover the cryptocurrency that he had sent to a supposed cryptocurrency investment fund that in fact was a

fraud scheme. This included retaining a blockchain investigation firm called CipherBlade and working with a criminal investigator from the United States Secret Service. If Lenny's cryptocurrency had remained in the self-custodied wallet to which Lenny unwittingly had sent it, that cryptocurrency would have been fully recoverable by federal law enforcement. Alternatively, because the stolen crypto was USDT, the entity that oversees the USDT blockchain (Tether Ltd.) could readily have frozen the USDT and issued replacement USDT to Lenny. But the stolen USDT did not remain in the self-custodied wallet. Because Binance allowed the criminal syndicate to open and freely utilize a Binance.com account, the criminal syndicate was able to quickly launder the criminal proceeds through the Binance.com exchange, specifically by transferring Lenny's cryptocurrency from the self-custodied wallet to multiple Binance.com accounts. This enabled the criminal syndicate to vanish into thin air with Lenny's hard-earned money.

7. If Binance had been operating in compliance with United States laws, rather than flouting them in order to aid and abet fraud schemes and money laundering, it would have identified that the criminal syndicate which scammed the Plaintiffs was using the Binance.com for illicit purposes and frozen the syndicate's Binance.com accounts, which in turn would have enabled United States law enforcement to seize the stolen cryptocurrency and return it to the Plaintiffs. But Binance was not complying with United States laws. Instead, with actual knowledge that fraud syndicates were looking to the Binance.com exchange for assistance with their schemes, Binance (as directed by Zhao) purposefully operated in a manner that facilitated, and aided and abetted, the fraud and money laundering. Binance and Zhao knew that criminal syndicates, such as the fraud syndicates that defrauded Lenny and his co-Plaintiffs, were using the Binance.com exchange in this manner to effectuate their frauds. Binance and Zhao knew that

they were facilitating and aiding and abetting those criminal syndicates' crimes, and they intended to do so. Binance and Zhao knew that Binance could put a stop to the criminal syndicates' activities, including by freezing Binance accounts that were being utilized for suspicious transactions, employing basic KYC to deter scammers, and reporting those illicit transactions to FinCEN. Binance and Zhao also knew that their conduct was itself a violation of federal criminal laws, including because it constituted aiding and abetting wire fraud and money laundering of pig butchering syndicates. But Binance and Zhao did not care. They cared more about the lucrative fees that Binance earned on every transaction that occurred on the Binance.com exchange, including money laundering transactions that Binance and Zhao knew were enabling the criminal syndicates to get away with their fraud schemes. They also cared about avoiding compliance with United States laws, including FinCEN registration requirements and anti-money laundering statutes, because it would impair their singular obsession with growing Binance's market share. In Zhao's own words, Binance had to "do everything to increase our market share, and nothing else." At the times relevant to this complaint, Binance's share of the worldwide cryptocurrency exchange market was estimated to be approximately 80%, which meant that unfettered access to and utilization of the Binance.com exchange was indispensable to fraud syndicates that needed to launder their stolen cryptocurrency assets on a centralized exchange in order to successfully complete their frauds.

8. Lenny Licht's story is unfortunately not unique. Binance's and Zhao's systematic, willful violations of federal criminal laws designed to keep financial markets safe and free from money laundering led to the exact result that Binance's own employees and executives—including Zhao—knew and predicted would result: criminal syndicates from around the world constructed fraud schemes that would and did use the Binance.com exchange as their proverbial

getaway cars, stealing massive amounts of money from thousands of people. Lenny Licht's co-Plaintiffs in this amended complaint are among the Defendants' victims, and their stories are summarized herein.

9. It is now time for Binance and Zhao, as well as their partner in crime BAM, to take responsibility, and to be held liable, for the devastating financial harm that their flagrantly unlawful racketeering activity caused to Plaintiffs.

II. THE PARTIES

10. Plaintiff Leonard Licht ("Lenny") is a United States citizen who resides in Plano, Texas. He resided in the United States at all times relevant to the complaint.

11. Plaintiff Zhengjun Cai is a Chinese citizen who resides in Irvine, California. She resided in the United States at all times relevant to the complaint.

12. Plaintiff Henry Chen is a United States citizen who resides in San Francisco, California. He resided in the United States at all times relevant to the complaint.

13. Plaintiff Daniel Chang is a United States citizen who resides in San Jose, California. He resided in the United States at all times relevant to the complaint.

14. Plaintiff Dominic Chow is a United States citizen who resides in Lexington, Massachusetts. He resided in the United States at all times relevant to the complaint.

15. Plaintiff Chengguo Dong is a United States citizen who resides in Fremont, California. He resided in the United States at all times relevant to the complaint.

16. Plaintiff Ihab W. Francis is United States citizen who resides in New City, New York. He resided in the United States at all times relevant to the complaint.

17. Plaintiff John Gordon is a United States citizen who resides in Miami, Florida. He resided in the United States at all times relevant to the complaint.

18. Plaintiff Dalton Green is a United States citizen who resides in Colorado Springs, Colorado. He resided in the United States at all times relevant to the complaint.

19. Plaintiff Michael Grilli is a United States citizen who resides in Palm Beach Gardens, Florida. He resided in the United States at all times relevant to the complaint.

20. Plaintiff Iraklis Karabassis is a United States citizen who resides in Miami, Florida. He resided in the United States at all times relevant to the complaint.

21. Plaintiff Nader Lobandi is a citizen of Iran who resides in Boston, Massachusetts. He resided in the United States at all times relevant to the complaint.

22. Plaintiff James Moskwa is a United States citizen who resides in Coventry, Rhode Island. He resided in the United States at all times relevant to the complaint.

23. Plaintiff Anh Nguyen is a United States citizen who resides in Anaheim, California. He resided in the United States at all times relevant to the complaint.

24. Plaintiff Brian Rothaus is a United States citizen who resides in Elkins Park, Pennsylvania. He resided in the United States at all times relevant to the complaint.

25. Plaintiff Gordon Shaylor is a United States citizen who resides in Henderson, Nevada. He resided in the United States at all times relevant to the complaint.

26. Plaintiff Richard Slavant is a United States citizen who resides in Monroe, Louisiana. He resided in the United States at all times relevant to the complaint.

27. Plaintiff Nathanial Thrailkill is a United States citizen who resides in Litchfield Park, Arizona. He resided in the United States at all times relevant to the complaint.

28. Plaintiff Jack Yao is a United States citizen who resides in San Diego, California. He resided in the United States at all times relevant to the complaint.

29. Plaintiff Jun Zhai is a United States citizen who resides in Seattle, Washington.

He resided in the United States at all times relevant to the complaint.

30. Defendant Binance Holdings Limited ("Binance") is a Cayman Islands company founded in or around 2017. Binance previously has touted itself as being essentially "headquarterless." Its founder and former CEO Changpeng Zhao stated in 2020, "Wherever I sit, is going to be the Binance office." In its November 2023 plea agreement, Binance admitted that, at least through October 2022, it "did business wholly or in substantial part within the United States." Binance also admitted that more Binance customers resided in the United States ***than any other country***, notwithstanding Binance's false public representations that United States customers exclusively utilized BAM's Binance.US platform and were blocked from using the Binance.com exchange.

31. Defendant BAM Trading Services, Inc. ("BAM") is a Delaware corporation headquartered either in Florida or Palo Alto, California. Doing business as Binance.US, BAM continuously and systematically transacts business throughout the United States, including in the District of Massachusetts. BAM is not a subsidiary of Binance, nor does BAM operate under a unified corporate structure with Binance. Indeed, in prior federal court actions, Binance and BAM have represented that BAM is not even a corporate affiliate of Binance.

32. Defendant Zhao is a Chinese-born citizen of Canada. Zhao is the founder and former CEO of Binance. Until at least 2022, Zhao owned approximately 90% of Binance's equity and BAM's equity and directed and controlled all of Binance's and BAM's corporate decisions, strategies, and conduct. Although Zhao spent time in the United States when he served his federal prison sentence for violations of the Bank Secrecy Act, on information and belief, Zhao's domicile is Dubai.

III. JURISDICTION AND VENUE

33. This court has subject matter jurisdiction pursuant to 18 U.S.C. § 1964(a) (RICO jurisdiction) and 28 U.S.C. § 1331 (federal question jurisdiction).

34. This court has general personal jurisdiction over Binance because, as Binance admitted in the Statement of Facts accompanying its November 2023 criminal plea, Binance "did business wholly or in substantial part within the United States" during the period 2017 through "at least October 2022." *See, e.g., Perkins v. Benguet Consolidated Mining Co., 342 U.S. 437 (1952); Helicopteros Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408 (1984); Northeast Structures, Inc. v. Wolfeboro Corinthian Yacht Club, Inc.,* 138 F.R.D. 345, 347 (D.R.I. 1991) ("A foreign corporation defendant may be subjected to the forum state's reach if its activities are 'substantial' or 'continuous and systematic [in the forum state],' even if these activities do not relate to the cause of action."); *see also Omni Video Games, Inc. v. Wing Co. Ltd., 754 F. Supp. 261, 263* (D. R.I. 1991) (holding that because the civil RICO statute provides for nationwide service of process, the defendant needs only to have had sufficient contacts with the United States for personal jurisdiction to apply). General personal jurisdiction over Binance is also warranted because at least until the end of 2022, at Zhao's express direction, Binance clandestinely maintained custody and control of the cryptocurrency assets that deposited, held, and traded on BAM's Binance.US platform, and maintained extensive ties to the operation of the Binance.US platform. General personal jurisdiction over Binance is also warranted because the Binance.com exchange was, during the relevant time period, maintained on Amazon Web Services ("AWS") servers located in the State of Washington, and those servers acted as Binance's figurative heart—as the Commodities Futures Trading Commission put it, "No AWS servers, no Binance.com exchange." In addition, a FinCEN investigation found that Binance

"maintained U.S.-based personnel and other operational touchpoints to the United States" during the time period relevant to this complaint. FinCEN found that Binance employed "more than 100 individuals who are based in the United States, including senior personnel, such as an advisor to [Zhao], several C-suite executives (e.g., the former Chief Business Officer, former Chief Strategy Officer, Chief Technology Officer), Global Director of Brand Marketing, and Vice President of Global Expansion Operations." FinCEN also found that Binance's most substantial market makers—that is, the persons and entities providing the daily trading liquidity that Binance needed for the Binance.com exchange to operate successfully—were based in the United States. Binance's unlawful U.S. operations included regularly and continuously soliciting and doing business with customers located in the Commonwealth of Massachusetts, including on information and belief Commonwealth-based market makers.

35. This court also has specific personal jurisdiction over Binance because the racketeering acts and conspiratorial conduct that are the predicates for the RICO causes of action against Binance, including the RICO conspiracy cause of action, include (1) Binance's purposeful availment of the United States cryptocurrency trading market, without registering with FinCEN as a money transmitting business, in violation of 18 U.S.C. § 1960(a), which also had the effect of making every transaction on the Binance.com exchange a violation of 18 U.S.C. § 1956(a)(1)(A)(i) (money laundering) by virtue of 18 U.S.C. § 1956(c)(7)(A)'s cross reference to 18 U.S.C § 1961(1) (defining "racketeering activity" to include violations of 18 USC § 1960); (2) Binance's formation of a RICO enterprise with BAM, a Delaware corporation headquartered in Florida or California, whose common purpose was to deceive United States law enforcement regarding Binance's connections to and exploitation of the United States market; (3) Binance instructing U.S.-based "VIP users" on how to use the Binance.com exchange while concealing

their United States location, in furtherance of the Binance/BAM enterprise's racketeering activity; (4) Binance's secret (and unlawful) solicitation, recruitment, and retention of U.S.-based "market makers," including high-frequency quantitative trading firms, that provided the Binance.com exchange with the substantial, sought-after liquidity that attracted criminal syndicates who needed a highly liquid laundering facility and cash-out point for their stolen cryptocurrency assets, which amounted to tens of millions, and more likely hundreds of millions or even billions, of stolen funds; (5) Binance's participation in the laundering of the cryptocurrency assets that criminal syndicates stole from Plaintiffs, many of them United States citizens or residents, by means of fraudulent representations; and (6) Binance's solicitation of U.S.-based "market makers" that provided the daily trading liquidity that served as the means by which money laundering schemes on the Binance.com exchange succeeded. Binance's unlawful U.S. operations, including regularly and continuously soliciting and doing business with customers located in the Commonwealth of Massachusetts, including on information and belief Commonwealth-based market makers.

36. The Court's personal jurisdiction over Binance can be established under Federal Rule of Civil Procedure 4(k)(2) because Binance has waived service of the complaint and is not subject to jurisdiction in any state's court of general jurisdiction, and asserted personal jurisdiction over Binance complies with the Due Process Clause in light of Binance's purposeful availment of the United States as a whole as described herein.

37. This court has general personal jurisdiction over BAM under 18 U.S.C. § 1965(a) because RICO provides for nationwide service of process and BAM conducts all or substantially all of its business in the United States, is incorporated in Delaware, and is headquartered in Florida or California. This court also has specific personal jurisdiction over BAM under the

Massachusetts long-arm statute because, as part of its role in concealing (and therefore facilitating) Binance's and Zhao's criminal conduct and deceiving U.S. regulators and law enforcement, BAM conducted substantial and continuous business operations in the Commonwealth, including regularly and continuously soliciting and doing business with, on information and belief, thousands of customers based in the Commonwealth. To successfully fulfill its role as Binance's regulatory "smokescreen," BAM's deceptive "kabuki theater" needed to include soliciting and doing business with customers in all major U.S. markets, including Massachusetts.

38. This court has general personal jurisdiction over Zhao because, as the CEO, control person, and approximately 90% equity holder of Binance during the relevant time period, as well as the Chairman of the Board of Directors and approximately 90% equity holder of BAM during the relevant time period, Zhao had continuous and systematic business contacts with the United States market that substantially enriched him personally.

39. This court also has specific personal jurisdiction over Zhao because (1) he participated in and directed the conduct of the various RICO enterprises' predicate racketeering acts that were specifically directed at the United States market (namely, the 18 U.S.C. 1960(a) violations), including by directing BAM's U.S.-based business operations and BAM's U.S.-based deceptions of United States regulators and law enforcement; and (2) he conspired in the laundering on the Binance.com exchange of cryptocurrency assets stolen from U.S. citizen plaintiffs by criminal syndicates by means of false representations sent via international wire communications.

40. The Court's personal jurisdiction over Zhao can be established under Federal Rule of Civil Procedure 4(k)(2) because Zhao has waived service of the complaint and is not

subject to jurisdiction in any state's court of general jurisdiction, and asserted personal jurisdiction over Zhao complies with the Due Process Clause in light of Zhao's purposeful availment of the United States as a whole as described herein.

41. Venue is proper in this judicial district under the RICO statute's venue provisions, 18 U.S.C. § 1965(a)-(b). First, BAM operates a U.S.-based crypto exchange whose nationwide operations include regularly and continuously soliciting, providing substantial services to, and profiting substantially from Massachusetts-based customers. BAM has registered with the Massachusetts Secretary of State's Office, stating that it operates a "Digital Asset Marketplace" in the Commonwealth; BAM also has designated registered agents in the Commonwealth. Second, as the SEC found after its lengthy investigation of Binance and Zhao, Binance and Zhao effectively "controlled" and were "integrally involved in" all of BAM's business operations, including its business operations in Massachusetts. Because Zhao owned virtually all of Binance's equity, and because Binance owned essentially all of BAM's equity, BAM's regular, substantial, and continuous business transactions in the United States, including all the business transactions that occurred in and exploited the market in Massachusetts, were effectively Binance's and Zhao's. Third, a substantial portion of Binance's systematic, unlawful U.S.-based operations—operations that it hid from United States regulators and law enforcement—occurred in or exploited the Massachusetts market, including regularly and continuously soliciting and providing services to Massachusetts-based customers and facilitating and settling cryptocurrency trades of Massachusetts customers. Binance's regular, substantial, and continuous business transactions in the Commonwealth essentially were the business transactions of Zhao, given that Zhao owned virtually all of Binance's equity and directed and tightly controlled Binance's decisions. Accordingly, 18 U.S.C. § 1965(a) vests this Court with venue over each of the

Defendants. Furthermore, to the extent 18 U.S.C. § 1965(a) vests this Court with venue over some but not all of the Defendants, the Court would be permitted to exercise venue over the remaining Defendants pursuant to 18 U.S.C. § 1965(b) in the interests of justice, particularly given that Binance and Zhao already "may be sued in any judicial district" pursuant to 28 U.S.C. § 1391(c)(3).

IV. FACTUAL ALLEGATIONS

A. Basic Summary of Cryptocurrency, the Blockchain, Self-Custodied Digital Wallets, and Cryptocurrency Exchanges

42. Cryptocurrency is a digital asset that exists only in electronic form, rather than as coins or bills. Cryptocurrency relies on cryptography to facilitate and validate transfers of the electronic currency from one party to another. Bitcoin, which was first introduced in a 2008 whitepaper,[1] is generally considered the first cryptocurrency asset system to have gained widespread adoption.

43. Transfers of cryptocurrencies are recorded on a "blockchain." The recordings are indelible, which means they cannot be deleted or altered. For each transfer, the blockchain records the "address"—a unique series of letters and numbers—of the transferor and transferee. The blockchain thus allows cryptocurrency to be traced and tracked.

44. A user's "address" is stored in a "digital wallet." As a general matter, there are two types of "wallets"—"self-custodied wallets" and "hosted wallets." A self-custodied wallet is a wallet that the user operates and controls. Storing cryptocurrency in a self-custodied wallet is analogous to putting cash under one's mattress or floorboard, and the "location" of a self-custodied wallet is the same as the location of the self-custodied wallet's owner—*i.e.* if someone is in the United States, their self-custodied wallet is in the United States. A hosted wallet, by

[1] Nakamoto, S. (2008) *Bitcoin: A peer-to-peer electronic cash system*.

contract, is owned, operated, and controlled by a centralized exchange, such as Binance.com. Storing cryptocurrency in a hosted wallet is analogous to depositing cash into a savings account at an FDIC-insured bank.

45. Since the release of Bitcoin ("BTC") in 2009, several related crypto-asset systems, including Ethereum, have been developed. Nearly all are built upon the same concept of a blockchain introduced by Bitcoin. Ethereum ("ETH") was first described in a whitepaper published in 2013 and was intended to overcome the limitations of Bitcoin by supporting the development of "smart contracts" that can encode an arbitrary set of rules for moving ether or other "tokens" between users.

46. Ethereum defines a standard smart contract format, called ERC-20,[2] that tokens may choose to implement. This is the primary smart contract at issue in this case.

47. A common use for ERC-20 tokens has been the issuance of crypto assets called "stablecoins." Stablecoins are a particular category of tokens that are correlated or "pegged" to another asset, such as the U.S. dollar. For example, USDT (commonly referred to as "Tether") is the stablecoin primarily at issue in this case. Issued by Tether Ltd., USDT is a popular stablecoin that is supposedly backed by at least an equal amount of U.S. dollars, such that one USDT is equivalent to one U.S. dollar. Stablecoins allow crypto users to purchase, hold, and transfer crypto assets without the volatility often associated with crypto assets like bitcoin and ether.

48. Crypto assets like BTC, ETH, and USDT may be converted to and from a country's legal tender, or between other types of crypto assets, through a "centralized exchange" such as Binance.com. Customers of a centralized exchange can deposit crypto assets or fiat

[2] ERC-20 Token Standard, https://web.archive.org/web/20231018074946/https://ethereum.org/en/developers/docs/standards/tokens/erc-20/ (Accessed: February 17, 2025.)

currency (*e.g.*, U.S. dollars) into their account at the exchange. The customer can then trade their deposited fiat or crypto assets for any of several other types of fiat currencies or crypto assets, transfer it to another account at the exchange, and/or withdraw it to another bank account or wallet address.

49. A person can hold cryptocurrency indefinitely in a self-custodied wallet. But, if the person wants to convert cryptocurrency to fiat currency in anonymous transactions with an unrelated third parties, the use of a centralized exchange is necessary.

B. The Plaintiffs, All of Whom Reside in the United States and Were Defrauded of USDT They Held in the United States, Collectively Lost Millions of Dollars to "Pig Butchering" Schemes That Utilized the Binance.com Exchange as a Necessary Component of the Schemes

50. A pig butchering scheme is a type of investment fraud that lures individuals into investing their money into a seemingly legitimate and profitable venture. The scheme often begins with an out-of-the-blue contact from a stranger via a social network platform, such as Facebook, Telegram or WhatsApp. At times, the scammer makes it appear that she meant to contact another person, but then, using the "mistaken" contact as an excuse, begins a conversation with the victim. Using fake or stolen images, as well as personal information scraped from the internet, the stranger convinces the victim that they have common friends or business contacts. After earning the victim's trust, the stranger convinces the victim to invest money into a supposedly safe but lucrative investment opportunity. After the victim invests an initial sum of money, the stranger creates false information showing that the investment is doing well, thereby convincing the victim to invest even more money. Eventually, the stranger disappears, and the victim learns that he "invested" in a fraud scheme and that his money has been stolen.

51. Pig butchering schemes involving cryptocurrency have become increasingly

common over the past decade. Criminal syndicates involved in pig butchering schemes prefer cryptocurrency because of the speed and anonymity of cryptocurrency transactions, as well as the ability to engage in transactions outside of the traditional (and highly regulated) banking system. Instead of convincing a victim to invest fiat currency into the supposed "investment," a criminal syndicate will convince the victim to purchase cryptocurrency on a well-known cryptocurrency exchange, such as Coinbase.com, and then to transfer that cryptocurrency to the "investment" entity, which is typically a self-custodied wallet controlled by the scammers. Scammers prefer to target U.S.-based victims because they are more likely to be wealthy.

52. For all the Plaintiffs, how the crypto was stolen from them was nearly identical. The scammers found these Plaintiffs on social media (Facebook, WhatsApp, Telegram) or a dating website. Plaintiffs here all had WhatsApp phone numbers with U.S. country and area codes and/or social media or dating app profiles that clearly indicated they were based in the United States. From there, the scammers would ingratiate themselves with their soon-to-be-victims, spending hours upon hours texting and communicating with the victims. During those long hours, the scammers would work diligently to develop a relationship of trust and confidence with the victims. The scammers generally probed their victims for details about their lives—where they lived, their relationship status, and their financial status.

53. Gradually, the scammers, who frequently posed as independently wealthy women looking for long-term relationships, would tell the victims about how they made money investing in cryptocurrency. The scammers would then teach their targets how to earn money just like they did. This was a multi-step process described below.

54. *First*, many of the victims already had accounts at U.S.-based centralized crypto exchanges, such as Coinbase.com. However, if the victim did not yet have a centralized

exchange account, the scammers instructed the victims to set up such an account. The victim would set up the account in his or her own name, providing the exchange with satisfactory KYC enabling the account to be opened. The KYC typically required at a centralized exchange—Kraken or Coinbase as examples—involved government-issued photographic identifications, which the exchange would then run through banking software to weed out potential criminals. To fund their crypto accounts, the victims typically sent wire transfers from their U.S.-based bank accounts to the centralized exchange, which would then credit the deposit to their accounts.

55. *Second*, the scammers typically instructed the victim to use his or her centralized exchange account to purchase USDT, which, as described above, is a stablecoin on the Ethereum blockchain. USDT typically trades on par with the US Dollar, meaning one USDT has the value of one U.S. Dollar.

56. *Third*, once the victim's centralized exchange account has USDT, the scammer will typically instruct the victim to create a self-custodied wallet and to transfer the USDT from his or her hosted wallet to his or her self-custodied wallet. As noted above, the location of the victim and the location of the victim's self-custodied wallet is one and the same.

57. *Fourth*, once the funds are in the victim's self-custodied wallet, scammers have found ways to move those funds to self-custodied wallets that the scammers control. At times, scammers would use malicious code that they would trick the victim into downloading into their self-custodied wallet; that malicious code would then allow the scammers to clandestinely move the USDT from the victim's self-custodied wallet to a self-custodied wallet controlled by the scammers. At other times, the scammers would use false representations to convince the victim to send the USDT to an address that in fact was a self-custodied wallet controlled by the scammers.

58. *Fifth*, the scammers ultimately transfer the stolen USDT to a hosted wallet on a centralized exchange, such as Binance.com, which is what enables the scammers to convert the USDT into fiat currency (typically U.S. dollars). Only after the USDT is converted to fiat currency is the underlying fraud successfully completed. Critically, the scammers generally do *not* send stolen USDT through other centralized exchanges before the funds arrive at the centralized exchange that they use to launder the USDT into fiat currency.

59. The directive by the scammers to purchase USDT is important to this case for multiple reasons. As a stablecoin with a value pegged to the U.S. dollar, USDT is one of the most widely used crypto-assets. Because of its high liquidity, USDT is easily tradeable on centralized exchanges, making it ideal for quick transactions and money laundering. Put simply, USDT is easy to move, and easy to convert into fiat currency and cash out—so long as the scammer is able to utilize a centralized exchange.

60. USDT also operates on a centralized model, meaning Tether Ltd. retains control mechanisms over its issued tokens. If USDT is reported stolen, the victim can report the incident to Tether Ltd. and provide Tether Ltd. with transaction hashes and evidence proving ownership. Tether Ltd. can then freeze the stolen tokens.[3] This is possible because Tether Ltd. maintains an administrative function over its smart contracts on supported blockchains like Ethereum. If a user reports a theft to law enforcement or Tether Ltd. directly and provides sufficient evidence, Tether Ltd. can blacklist the address holding the stolen USDT, preventing further transfers.[4] In some cases, Tether Ltd. can even "burn" the blacklisted USDT and issue replacement tokens to the

[3] Tether Ltd. developed an ability to freeze and blacklist USDT at least as early as 2017. *See, e.g.*, https://cryptoslate.com/tether-freezes-three-ethereum-addresses-holding-150-million-in-usdt/; https://cryptobriefing.com/tether-can-freeze-destroy-your-usdt/

[4] On December 15, 2023, Tether Ltd. sent a letter to a US Senator and Congressman explaining that, as of that date, Tether Ltd. had frozen, on behalf of US law enforcement alone, approximately 326 wallets totaling approximately USDT 435 million. *See* https://tinyurl.com/5c4csea5

rightful owners—effectively nullifying the stolen funds, depriving the thief of all their value, and making the victim whole via replacement tokens.

61. In November 2023, for example, Tether Ltd. worked with the Department of Justice to freeze $225 million of USDT linked to pig butchering syndicates that used their fraud schemes to finance human trafficking activities. Tether Ltd. was alerted to the fraud by a centralized exchange that, by that time, was making diligent efforts to comply with European Union's strict anti-money laundering laws.

62. However, if a centralized exchange allows the scammers unfettered ability to transfer the stolen USDT to accounts they maintain on that centralized exchange, this impedes the ability of Tether Ltd. to blacklist and freeze the stolen USDT. Accordingly, once deposited into accounts on a centralized exchange that is not complying with anti-money laundering laws and allowing money laundering activities to occur, the USDT is typically out of reach of Tether Ltd. And if the centralized exchange allows the scammers to exchange the USDT for fiat currency and then withdraw the fiat currency to foreign bank accounts, the scammers are able to successfully complete their underlying fraud scheme. This makes a centralized exchange's permissive treatment of fraud syndicates an indispensable component of the fraud syndicates' success.

C. Binance and Zhao Knowingly and Willfully Aided and Abetted Pig Butchering Syndicates' Wire Frauds and Money Laundering

63. Because cryptocurrencies are built on public blockchains, cryptocurrency transactions can be tracked and traced using computer forensic analysis and off-the-shelf software. Accordingly, law enforcement will, as a general matter, be able to locate and seize the stolen assets from the criminals and return the assets to their rightful owners as long as the crypto is not exchanged for fiat in a centralized exchange and cashed out. Or, as described, Tether Ltd.

can freeze and blacklist USDT and re-issue that stolen USDT to the victim. For these reasons, keeping USDT in a self-custodied wallet is not a realistic option for the scammers—if they did, the stolen USDT eventually would be found and seized by the authorities or destroyed by Tether Ltd., and the victim would be made whole. As a result, it is an indispensable part of pig butchering for a criminal syndicate to launder the cryptocurrency that it has stolen from the scheme's victims and use a centralized exchange such as Binance to *convert it to fiat currency*. Put another way, to reap the benefits of their fraud and retain their ill-gotten gains, scammers need to launder the funds on an exchange such as Binance.com and convert the USDT (which is a digital asset and not cash) into fiat currency, where it can be withdrawn and deposited into a bank account. Simply put, the victim's financial injury becomes permanent only when the fraudsters successfully launder their stolen funds on an exchange such as Binance.com.

64. Criminal syndicates' ability to rapidly convert stolen cryptocurrency into untraceable fiat currency depends upon their unfettered ability to utilize cryptocurrency exchanges with substantial liquidity. If a criminal syndicate is unable to utilize such exchanges, it is difficult if not impossible for the syndicate to cash out of their schemes—instead, the cryptocurrency assets they stole from innocent victims will eventually be tracked, traced, and seized by law enforcement. In addition, if a cryptocurrency exchange flags a criminal syndicate's transactions as suspicious, freezes the syndicate's account, and reports the syndicate's transactions to FinCEN—as would be required by the Bank Secrecy Act—the syndicate will be prevented from cashing out of their schemes, and law enforcement can more rapidly seize the stolen assets and return them to the victims.

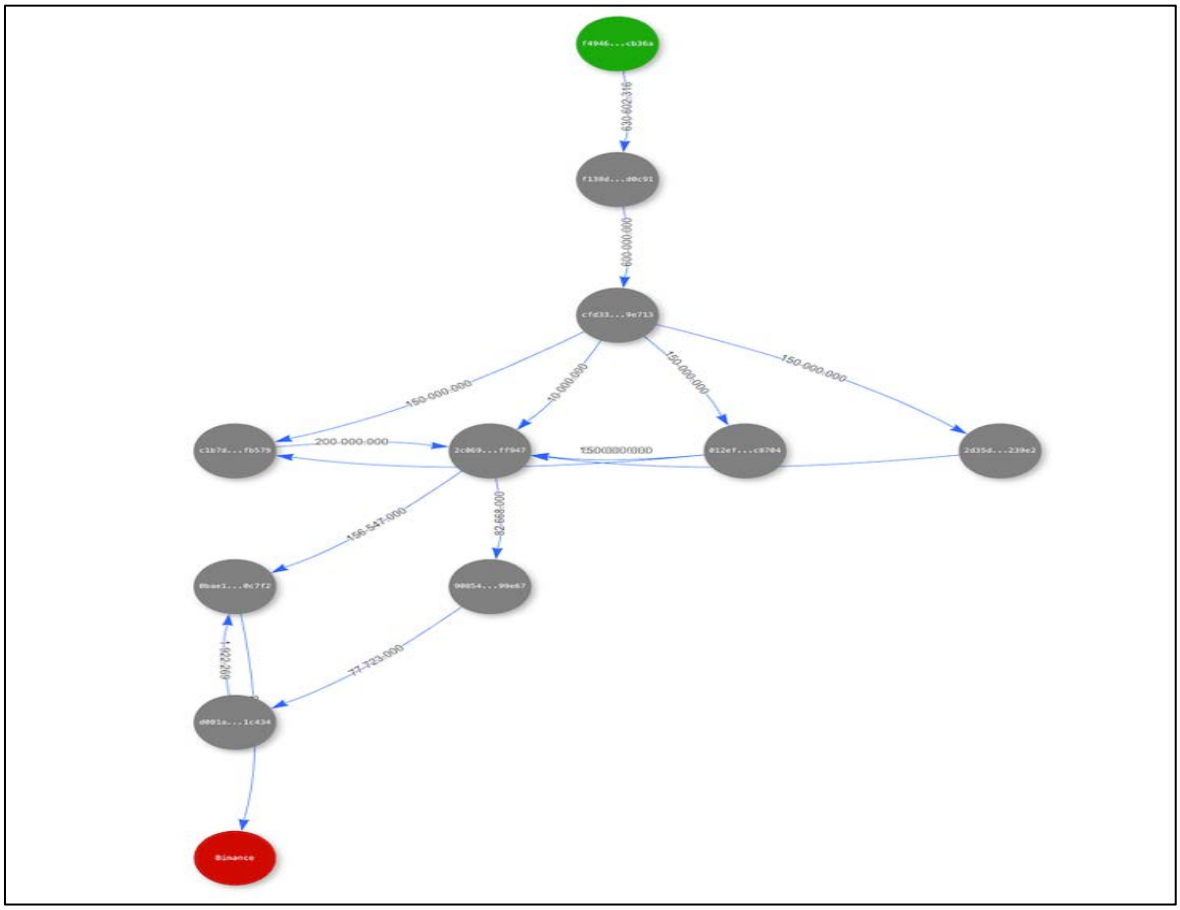
65. Conversely, if a cryptocurrency exchange with substantial liquidity knowingly and willfully fails to comply with the Bank Secrecy Act and instead allows criminal syndicates

to use the exchange as a laundering facility and cash-out point—which is what Binance and Zhao, with the assistance of BAM, have admitted to doing—criminal syndicates can easily cash out of the pig butchering scheme, leaving the victims completely unable to recover their stolen assets.

66. The pattern of inflows to fraudsters' Binance accounts, coupled with the accounts' cash-out activities, were themselves tell-tale signs that those Binance accounts were being used to launder and cash out of illicit cryptocurrency assets. The illustrative examples described below, which are consistent with the facts for all the Plaintiffs, illustrate the patterns.

Zhengjun Cai's Loss

67. As discussed below, Cai, a resident of California, had nearly $740,000 of USDT stolen from her self-custodied wallet. As set forth in the diagram below, after the USDT was stolen from Cai's self-custodied wallet (colored in green), it took multiple hops through self-custodied wallet controlled by the scammers (colored in gray). The scammers then deposited approximately $300,000 of the USDT into the scammers' custodial account on the Binance.com exchange (colored in red). None of the USDT passed through a centralized exchange before being deposited in the Binance.com account.



68. Notably, a forensic blockchain analysis shows that the scammers were unable to utilize for meaningful laundering purposes any centralized exchange that was complying with U.S. anti-money laundering rules at the time. The scammers apparently tried to utilize the Coinbase.com exchange, which was operating the KYC program required by the Bank Secrecy Act. Tellingly, the scammers were only able to deposit $982 of USDT in the Coinbase account.

69. The activity in the scammers' Binance.com account had all the telltale signs of money laundering. Etherscan, a publicly available blockchain tracing tool, shows that one of the self-custodied wallets (the wallet with the 0x0bAE1184 address) that the scammers used in their fraud against Cai first began depositing large quantities of USDT in the scammers' Binance.com account in early 2022. These deposits to the Binance.com account would be made within hours

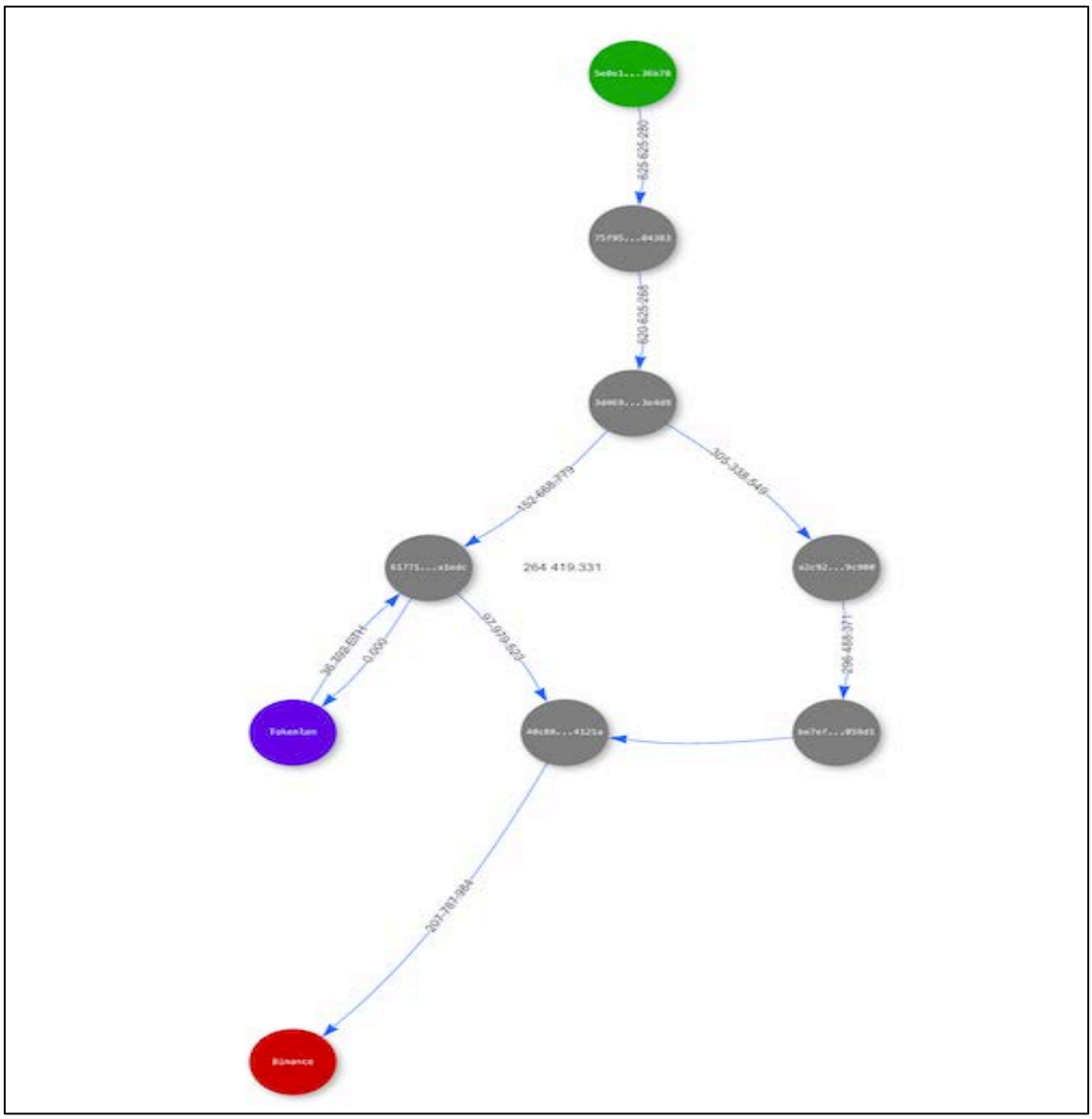
of the self-custodied wallet's receipt of the USDT.

2022-01-25 16:08:00	0x90854eBA...0E2699e67	IN	0x0bAE1184...30340c7f2	50,000	Tether USD (USDT)
2022-01-25 9:21:19	0x0bAE1184...30340c7f2	OUT	Binance Dep: 0x860d6...	55,011	Tether USD (USDT)
2022-01-25 7:55:16	0x391400F2...9Ae36BFaC	IN	0x0bAE1184...30340c7f2	4,944	Tether USD (USDT)
2022-01-25 4:18:45	0x0bAE1184...30340c7f2	OUT	Binance Dep: 0x860d6...	50,000	Tether USD (USDT)
2022-01-25 3:26:44	0x90854eBA...0E2699e67	IN	0x0bAE1184...30340c7f2	100,000	Tether USD (USDT)
2022-01-23 4:02:39	0x0bAE1184...30340c7f2	OUT	Binance Dep: 0x860d6...	9,400	Tether USD (USDT)
2022-01-22 13:38:03	0x0bAE1184...30340c7f2	OUT	Binance Dep: 0x860d6...	40,000	Tether USD (USDT)

70. This pattern continued almost daily for months. It total, over an approximately 3-month period, more than $6 million passed from this single self-custodied wallet controlled by scammers to the scammers' Binance.com account.

John Gordon's Loss

71. Plaintiff John Gordon had nearly $625,000 in USDT stolen from his self-custodied wallet by scammers. The stolen USDT went from Gordon's wallet (colored in green) to a self-custodied wallet controlled by the scammers (the top oval colored in gray). The scammers then passed the USDT through additional self-custodied wallets that they controlled (also colored in gray), and then *84% of that stolen USDT* was deposited into their Binance.com account (colored in red).



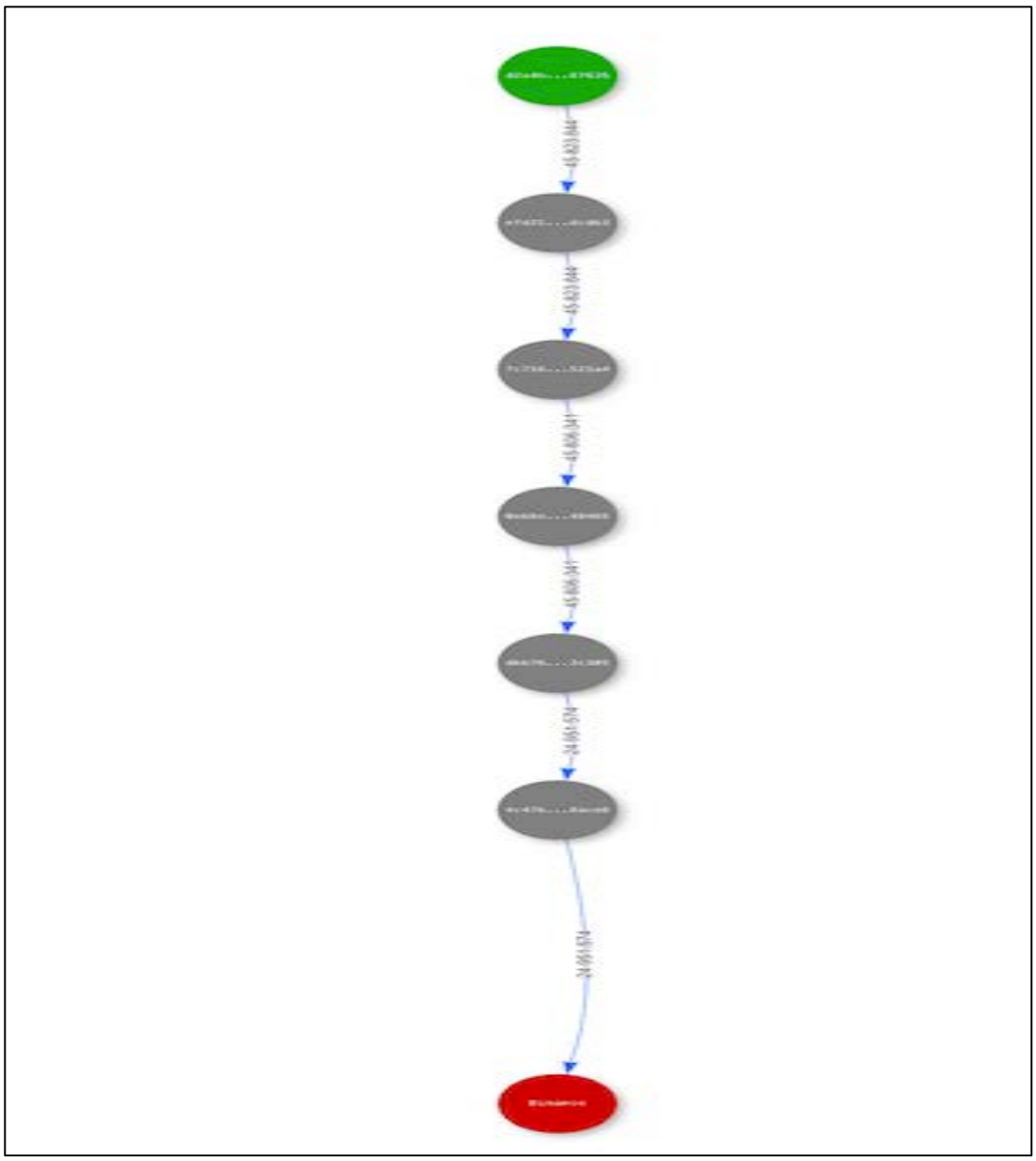
72. Further, similar to the fraud against Cai, one of the self-custodied wallets (the wallet with the 0x40C88C82 address) used by the scammers sent hundreds of thousands of dollars' worth of USDT to the scammers' Binance.com account almost immediately after the funds were received by the 0x40C88C82 wallet. These telltale signs of money laundering were publicly available blockchain information that any competent KYC program would have red-flagged. The fact that Binance allowed the scammers to make these deposits in a completely unfettered manner is evidence from which one can reasonably infer that Binance was knowingly

and willfully allowing the scammers to utilize the Binance.com exchange to complete their fraud schemes.

2022-07-26 5:11:43	0x40C88C82...8cbf4121a	OUT	Binance Dep: 0x7185E...	116,436	Tether USD (USDT)
2022-07-26 5:08:10	0x3D7Eea65...f02aF0904	IN	0x40C88C82...8cbf4121a	116,279	Tether USD (USDT)
2022-07-25 11:59:19	0xaAdA21Cb...82E2d142F	IN	0x40C88C82...8cbf4121a	57	Tether USD (USDT)
2022-07-25 8:20:59	0x4edd6B9A...5aDC18289	IN	0x40C88C82...8cbf4121a	100	Tether USD (USDT)
2022-07-21 11:51:53	0x40C88C82...8cbf4121a	OUT	Binance Dep: 0x7185E...	120,000	Tether USD (USDT)
2022-07-21 11:45:46	0x40C88C82...8cbf4121a	OUT	Binance Dep: 0x7185E...	100,000	Tether USD (USDT)
2022-07-21 11:36:50	0x40C88C82...8cbf4121a	OUT	Binance Dep: 0x7185E...	100,000	Tether USD (USDT)
2022-07-21 11:25:02	0xa6a63e61...95a10fcd2	IN	0x40C88C82...8cbf4121a	320,000	Tether USD (USDT)

Gordon Shaylor's Loss

73. As a final example, Plaintiff Gordon Shaylor had more than $670,000 in USDT stolen from his self-custodied wallet. The USDT went from Shaylor's self-custodied wallet (colored in green) to a self-custodied wallet controlled by the scammers (the top oval colored in gray). The scammers then passed the USDT through a chain of other self-custodied wallets (the other ovals colored in gray). A self-custodied wallet then transferred the USDT to their Binance.com account (colored in red). One example of this transfer is set forth in the chart below:



74. Approximately 30% of Shaylor's stolen USDT was deposited into the scammers' Binance.com account, with the remainder of the USDT deposited into accounts at other centralized exchanges that were not complying with U.S. anti-money laundering rules at the time (Huobi, OKX, and FTX). As with Cai and Gordon, the self-custodied wallet that the scammers used to transfer the stolen USDT to Binance had all the hallmarks of money laundering:

Date Time (UTC)	From		To	Amount	Token
2022-05-10 17:59:43	0x0301D347...35482af48	OUT	Binance Dep: 0xceBaB...	52,156	Tether USD (USDT)
2022-05-10 17:54:04	0x0301D347...35482af48	OUT	Binance Dep: 0xceBaB...	80,000	Tether USD (USDT)
2022-05-10 17:34:46	0x0301D347...35482af48	OUT	Binance Dep: 0xceBaB...	80,000	Tether USD (USDT)
2022-05-10 17:20:12	0x0301D347...35482af48	OUT	Binance Dep: 0xceBaB...	80,000	Tether USD (USDT)
2022-05-10 16:56:56	0x0301D347...35482af48	OUT	Gate.io Dep: 0x39F5Fb....	20,000	Tether USD (USDT)
2022-05-10 16:48:50	0x0301D347...35482af48	OUT	Binance Dep: 0xceBaB...	80,000	Tether USD (USDT)
2022-05-10 13:19:16	0x93EB5645...b7Fef8578	IN	0x0301D347...35482af48	392,155	Tether USD (USDT)

76. Once again, the fact that Binance allowed these transactions to occur allows for a reasonable inference that Binance and its puppeteer Zhao were knowingly and willfully facilitating and aiding and abetting the fraud schemes that depended upon money laundering on a centralized cryptocurrency exchange.

77. If Binance had registered itself with FinCEN as a money transmitting business, rather than illegally operate as an unregistered money transmitting business in violation of 18 U.S.C. § 1960(a), Binance would have been required to comply, and would have complied with, the Bank Secrecy Act's anti-money laundering provisions. And had Binance complied with the Bank Secrecy Act's anti-money laundering requirements, scammers would not have been able to successfully use the Binance.com exchange to launder the USDT stolen from the Plaintiffs.

78. Notably, in the few months immediately leading up to its November 2023 criminal plea, Binance started publicly touting its newfound dedication to legal compliance, including its work with law enforcement to crack down on pig butchering schemes and to help victims recover cryptocurrency assets that had been stolen from them. On August 23, 2023, for example, Binance issued a press release on its website entitled, "Binance Reports a 100% Rise in

Pig Butchering Scams and Shares Tip to Prevent Them." In the press release, Binance touted its ability to use blockchain forensics to "identify and fight illicit actors in the crypto ecosystem," to "prevent criminals from benefitting from their ill-gotten gains," and to take "swift action by identifying and restricting the flow of illicit funds through the [Binance] platform." Binance stated that its "proactive investigation and monitoring work" enabled law enforcement to "recover funds" for victims of pig butchering schemes that attempted to utilize the Binance.com exchange as a laundering facility and cash-out point. This essentially amounts to an admission by Binance that registering with FinCEN and complying with United States anti-money laundering laws equips Binance to do the very thing that would have enabled Lenny to recover the USDT that was stolen from him—identify suspicious transactions and users, freeze the accounts at issue, and facilitate law enforcement's seizure of the assets in the accounts and the return of those assets to their rightful owners. Indeed, Binance's Chief Communications Officer Brian Hillmann publicly stated in the summer of 2022 that "what's important to note is not where the funds come from—as crypto deposits cannot be blocked—but what we do after the funds are deposited," which would include ensuring that "any illegal funds are tracked, frozen, recovered and/or returned to their rightful owner."

79. Notably, in the 15 months since Binance began complying in earnest with the Bank Secrecy Act's anti-money laundering requirements, United States law enforcement authorities have seen a dramatic increase in the success of their efforts to recover cryptocurrency assets stolen from innocent victims by international fraud syndicates. In April 2023, for example, the United States Department of Justice announced that it had seized $112 million in cryptocurrency that one or more criminal syndicates had stolen from victims using pig butchering schemes. Using cryptography and forensic analysis, the Department of Justice and its

forensic experts were able to unwind a huge, commingled network of transactions and follow the proceeds of the frauds to cash- out points at cryptocurrency exchanges, enabling the government to seize the proceeds before the criminals were able to cash out. This demonstrates that Binance's flagrant violation of FinCEN registration requirements and United States anti-money laundering laws between 2017 and October 2022 had real-world consequences for everyday people like Plaintiffs, who had fallen prey to pig butchering schemes committed by international crime syndicates.

80. Unfortunately for the Plaintiffs, during the time period that their syndicates was utilizing the Binance.com exchange as a laundering facility for the USDT that it stole from them, Binance, as described below, was still flagrantly violating 18 U.S.C. § 1960 and the Bank Secrecy Act, including Bank Secrecy Act's anti-money laundering requirements, and continuing to ensure that its exchange was hospitable to and used by criminals whose illicit transactions were increasing Binance's profits. Binance also routinely and purposefully ignored or refused to respond to victims' proactive requests to freeze Binance accounts that forensic analyses showed were associated with the fraud schemes that stole the victims' cryptocurrency assets.

D. Binance and Zhao Have Admitted to Criminal Conduct That Constitutes RICO Predicates in Their Own Right and That Aided and Abetted the Wire Frauds and Money Laundering That Injured the Plaintiffs

81. Starting at least as early as August 2017 and continuing until at least October 2022, Binance—led by its founder, owner, and CEO Changpeng Zhao, and certain of its officers, directors, employees, and agents—knowingly failed to register with FinCEN as a money transmitting business, in violation of 18 U.S.C. § 1960, and willfully violated the Bank Secrecy Act by failing to implement and maintain an effective anti-money laundering program.

82. Binance's violations of federal criminal law were part of a deliberate and

calculated effort to profit from the United States cryptocurrency market without implementing controls required by United States law.

83. The Defendants knew that the Binance.com exchange was facilitating and aiding and abetting the crimes of fraud syndicates, including fraud schemes and money laundering that were causing financial injury to American citizens, and they intended the Binance.com exchange to operate in this fashion because it increased Binance's profits.

84. During the August 2017 through October 2022 period, Binance operated wholly or in substantial part in the United States by serving a large number of United States users. Because of the nature of the Binance.com exchange, Binance was operating an unlicensed money transmitting business in violation of United States law. Binance operated as an unlicensed money transmitting business in part to prevent United States regulators from discovering that Binance was facilitating billions of dollars of cryptocurrency transactions on behalf of its customers without implementing appropriate "know your customer" procedures or conducting adequate transaction monitoring.[5]

85. Due to Binance's willful failure to implement an effective anti-money laundering program, Binance processed transactions by users who operated illicit mixing services and were laundering proceeds of darknet market transactions, hacks, ransomware, and scams (including pig butchering scams).

86. Binance users could store and trade value in the form of virtual assets, including

[5] Nearly every allegation in this subsection of the complaint is a verbatim or near-verbatim copy of the respective Statements of Facts appended to Binance's and Zhao's November 2023 1plea agreements. Having agreed to the Statements of Facts as part of their pleas, Binance and Zhao should be precluded from collaterally challenging the factual allegations in this subsection of the complaint, at least insofar as the factual allegations track those in the plea agreements' Statements of Facts. *See, e.g., Trinidad v. City of Boston, No. 07-CV-011679-DPW, 2010 U.S. Dist. LEXIS 71900, at *22 (D. Mass. July 16, 2010)* ("Federal Courts of Appeals, including the First Circuit, applying federal law, have accorded preclusive effect to federal guilty pleas in subsequent federal civil proceedings.").

cryptocurrency, in accounts (or "wallets") maintained by Binance. When a user opened a Binance account, Binance assigned them a custodial virtual currency wallet—i.e., a wallet in Binance's custody that allowed the user to conduct transactions on the platform, including transferring funds to other Binance users or accounts or to external virtual currency wallets, and to convert cryptocurrency into fiat currency that could then be transferred into traditional bank accounts (including accounts at wholly foreign banks outside the purview of United States regulatory authorities) or otherwise withdrawn.

87. Binance charged its users fees on every transaction that the users conducted on Binance. Binance thus had an economic incentive to allow, and profited from allowing, illicit transactions on the Binance.com exchange. Binance chose not to comply with United States legal and regulatory requirements, including anti-money laundering requirements, because it determined that doing so would limit the scale and speed of its revenue growth.

88. Because Binance was operating a money transmitting business, it was required to register with FinCEN, or risk criminal penalties under 18 U.S.C. § 1960. Binance knew it was operating a money transmitting business required to be registered with FinCEN under 18 U.S.C. § 1960(a). Binance, however, chose not to register with FinCEN, meaning that it was willfully operating in violation of 18 U.S.C. § 1960(a) every single day until at least October 2022. Because Binance was in violation of 18 U.S.C. § 1960(a), every transaction that Binance conducted on the Binance.com exchange during the relevant time period—which is to say, every transaction that occurred on the Binance.com exchange during the relevant time period—also constituted a violation of 18 U.S.C. § 1956(a)(1)(A)(i) by virtue of 18 U.S.C. § 1956(c)(7)(A)'s cross-reference to 18 U.S.C. § 1961(1).

89. Binance also failed to comply with the Bank Secrecy Act's anti-money laundering

provisions, which applied to Binance because it was operating a money transmitting business. The anti-money laundering provisions that Binance flouted included provisions designed to prevent a money transmitting business from being used to facilitate money laundering and the financing of terrorist activities, as well as provisions requiring the filing of suspicious activity reports with FinCEN and monitoring for suspicious transactions. Binance and Zhao knowingly and willfully did not systematically monitor transactions on Binance's exchange, as required by the Bank Secrecy Act's anti-money laundering provisions.

90. Binance and Zhao knew that, by not monitoring for suspicious transactions and not conducting "Know Your Customer" diligence as required by the Bank Secrecy Act, they were facilitating and aiding and abetting criminal activity, including fraud schemes that were causing financial injury to American citizens. A Binance executive wrote to a colleague that Binance should create "a banner" stating, "[I]s washing drug money too hard these days[?] [C]ome to binance[,] we got cake for you." This was an acknowledgment that Binance was tacitly conspiring with criminals whom Binance and Zhao knew, or consciously avoided learning, were utilizing the Binance cryptocurrency exchange as a laundering facility and cash-out point for ill-gotten proceeds stolen from fraud victims.

91. Due to Binance's failure to implement an effective anti-money laundering program, illicit actors used Binance's exchange in various illicit ways, including: operating mixing services that obfuscated the source and ownership of cryptocurrency; transacting illicit proceeds from ransomware variants; and moving proceeds of darknet market transactions, exchange hacks, and various internet-related scams including pig butchering schemes. For example, between August 2017 and April 2022, there were direct transfers of approximately $106 million in bitcoin to Binance.com wallets from Hydra, a popular Russian darknet

marketplace frequently utilized by criminals that facilitated the sale of illegal goods and services. These transfers occurred over time to a relatively small number of unique addresses, which indicates "cash out" activity by a repeat Hydra user, such as a vendor selling illicit goods or services. Similarly, from February 2018 to May 2019, Binance processed more than $275 million in deposits and more than $273 million in withdrawals from BestMixer, which was one of the largest cryptocurrency mixers in the world until it was shut down by Dutch authorities in May 2019. The forensics firm Chainalysis, which the United States government routinely hires to track illegal cryptocurrency transaction flow, concluded in a 2020 report that in 2019 alone the Binance.com exchange was used as a laundering facility for $770 million in illicit funds. A Reuters investigation found that from 2017 to 2021 Binance processed transactions totaling at least $2.35 billion stemming from hacks, investment frauds, and illegal drug sales.

92. Binance and Zhao knew that some of these "VIP users"—a term Binance used for customers who conducted substantial transaction volumes on the Binance.com exchange—were illicit actors or "high-risk users." In some instances, Binance and Zhao knowingly and willfully chose not to take any adverse action against such users' accounts, instead allowing these bad actors to continue to access and utilize the Binance.com exchange. In other instances, Binance engaged in sham compliance efforts, "shutting down" the users' accounts but then immediately allowing the users to open up new accounts and, incredibly, providing those users instructions on how to avoid raising red flags with their future transactions.

93. To conceal its failure to comply with United States anti-money laundering requirements, and to conceal that it was operating an illegal money transmitting business without registering with FinCEN, Binance and Zhao formed in or around June 2019 a new entity that they publicly called Binance.US. Binance.US was the d/b/a identity of a Delaware corporation

called BAM Trading Services, which was at least 90% owned by Zhao. In or around June 2019, Binance.US registered itself with FinCEN as a money transmitting business and made at least superficial efforts to comply with the Bank Secrecy Act's anti-money laundering provisions. Binance touted Binance.US as the cryptocurrency exchange to which U.S.-based customers would be directed. Binance did this, however, specifically and willfully to create a false and misleading impression that Binance itself was not servicing U.S.-based customers and, therefore, was not subject to United States laws including the Bank Secrecy Act. Binance, BAM, and Zhao knew, however, that the Binance.com exchange—which remained unregistered with FinCEN and was not attempting to comply (let alone actually complying) with the Bank Secrecy Act's anti-money laundering provisions—maintained a substantial United States user base.

94. Binance's founder and CEO Zhao created and launched Binance.US because he knew that the Binance.US entity, indirectly controlled by Binance, would become the focus of United States law enforcement and regulatory authorities, which would allow Binance itself to continue to profit from the United States market without actually complying with United States laws. In other words, Binance.US was, at least in part, created to provide a legal and regulatory smokescreen that would distract United States regulatory and law enforcement authorities from Binance itself. In Zhao's own words, the "goal" behind Binance.US was "to make the U.S. regulatory authorities not trouble us." BAM conspired with Zhao's and Binance's plan to use Binance.US as a smokescreen that would enable Binance to continue to flout 18 U.S.C. § 1960(a) and the Bank Secrecy Act without drawing scrutiny from United States regulators and law enforcement. At least through October 2022, BAM agreed to, and did, falsely represent to the public, United States regulators, and United States law enforcement that all U.S.-based customers were being routed to the Binance.US exchange and were prohibited from utilizing the

Binance.com exchange.

95. Binance and Zhao knew that, so long as Binance continued to have substantial business connections with the United States, Binance would be required to comply with United States registration requirements and the Bank Secrecy Act, notwithstanding the existence of Binance.US.

96. Binance and Zhao knew that its high-volume "VIP users"—which included VIP users whom Binance and Zhao knew, or consciously avoided learning, were engaged in illicit activities and using the Binance.com exchange to launder criminal proceeds—accounted for approximately 70% of the company's transaction revenues, and it knew that approximately 30% of those VIP users were based in the United States. After launching Binance.US, Binance executives and senior leaders, including CEO Zhao, encouraged these VIP users—including the VIP users based in the United States—to continue to utilize the Binance.com exchange (rather than Binance.US) and to conceal and obfuscate their United States connections. During a conference call on or around June 25, 2019, Binance employees and executives told CEO Zhao that they were contacting United States VIP users "offline" through direct phone calls so that Binance would "leave no trace." A Binance executive acknowledged that Binance's plan to retain its VIP users on the Binance platform was an "international circumvention of [Know Your Customer] rules." Nevertheless, Binance continued to take steps in furtherance of that plan, including using a "script" that Binance representatives would use with VIP users that Binance and Zhao knew were based in the United States. The script included instructions to the VIP user on how the user could conceal his United States location by, among other things, altering the IP address of the computer that the user used to log in to Binance.com.

97. Approximately one year after Binance.US launched, Binance and Zhao knew that

approximately 16% of Binance.com customers were based in the United States—***more than any other country***. In October 2020, Binance executives altered internal company reports to conceal this fact. Specifically, whereas company reports before October 2020 specifically identified the percentage of Binance.com customers who were based in the United States, beginning in October 2020, those same reports recategorized U.S.-based customers with the label "UNKWN."

98. According to Binance's own transaction data, United States users conducted trillions of dollars in transactions on the Binance.com exchange between August 2017 and October 2022—transactions that generated approximately $1.6 billion in transaction fees (pure profit) for Binance.

99. By concealing that the Binance.com exchange was serving a substantial percentage of U.S.-based customers, Binance illegally avoided registering with FinCEN and thereby illegally avoided complying with the Bank Secrecy Act's anti-money laundering requirements. Had Binance complied with those federal laws, Binance would have been required to conduct "Know Your Customer" diligence on *all* Binance.com customers—not just those customers based in the United States. It also would have been required to monitor the Binance.com platform for suspicious transactions and to notify FinCEN of suspicious transactions. Binance did none of these things, because it knew that being hospitable and attractive to illicit actors and eschewing anti-money laundering obligations increased the size of Binance's customer base, increased Binance's transaction volume, and therefore enhanced Binance's profits and Zhao's personal fortune. Indeed, Binance never filed a suspicious activity report with FinCEN, despite knowing, consciously avoiding learning, and making themselves willfully blind to the fact that criminal syndicates were using the Binance.com exchange to facilitate their criminal schemes, specifically by using the Binance cryptocurrency exchange to

launder stolen cryptocurrency assets and convert those stolen assets into fiat currency. According to FinCEN's investigatory findings, Binance's former Chief Compliance Officer reported to other Binance personnel that the senior management policy was to never report any suspicious transactions. Indeed, FinCEN found during its investigation that Binance elected to allow customers to continue to use the Binance.com exchange for transactions that a senior Binance manager described as "standard money laundering."

100. Binance, through its conduct and willful inaction, knowingly and willfully facilitated and at least indirectly participated in the fraud schemes that utilized the Binance cryptocurrency exchange as a laundering facility and cash-out point. Moreover, to the extent Binance and Zhao knew, consciously avoided learning, or made themselves willfully blind to the fact that certain of its customers were engaged in illicit money laundering on the Binance cryptocurrency exchange, Binance itself knowingly engaged in financial transactions in violation of 18 U.S.C. § 1956(a)(1)(A)-(B), because any financial transaction conducted through a Binance account by definition was a transaction involving Binance.

101. As early as September 2018, Binance executives acknowledged that Binance had "[n]othing . . . in place" to review high-volume accounts for suspicious activity and that many transactions were occurring on Binance.com that "in [the] aml [anti-money laundering] world" would be flagged for money laundering risks. Binance's CEO Zhao, however, said that he did "see a need to" comply with anti-money laundering rules and that it was "better to ask for forgiveness than permission." CEO Zhao, and therefore Binance, believed that subjecting Binance's customers to a "Know Your Customer" process compliant with United States law, monitoring transactions for suspicious activity as required by the Bank Secrecy Act, and reporting suspicious transactions to FinCEN as required by the Bank Secrecy Act, would mean

that some customers would choose not to use Binance and that others would be rejected or flagged by the compliance process, both of which would interfere with Binance's efforts to gain market share and increase its profits. This led one member of Binance's so-called compliance department to write, "[W]e need a banner '[I]s washing drug money too hard these days[?] [C]ome to binance[,] we got cake for you.'" This compliance employee's statement was essentially an admission that a natural and foreseeable consequence of Binance's flagrant violation of 18 U.S.C. § 1960(a) and the concomitant requirement to comply with the Bank Secrecy Act's anti-money laundering provisions was that Binance was inviting criminals to use the exchange as a laundering facility and cash-out point for its illicit cryptocurrency proceeds.

102. Brian Shroder became the CEO of Binance.US in August 2021, shortly after the Cambodian syndicate's fraud scheme against Lenny occurred. Although Zhao in fact controlled and directed BAM's and Binance.US's conduct, including BAM's efforts to mislead United States regulators and law enforcement regarding Binance's clandestine exploitation of the United States trading market in violation of 18 U.S.C. § 1960(a), Shroder agreed with Zhao that BAM should participate in and conspire with Binance's and Zhao's criminal scheme. Shroder's brother Matt worked for Binance as the head of Binance's Global Expansion Operations team. Shroder was aware, at the time that he became the Binance.US CEO, that Binance was continuing to operate in the United States market illegally, in violation of 18 U.S.C. § 1960. Shroder, however, agreed with Zhao that BAM would maintain the public-facing position that all U.S.-based customers were restricted to using the Binance.US exchange, which had registered with FinCEN and was endeavoring to comply with United States anti-money laundering laws. Shroder knew that this public-facing position was false. Shroder also continued to publicly tout that Binance.US was "regulatorily compliant," despite knowing that Binance.US in fact was intended

by Zhao to be a smokescreen to distract United States regulatory agencies and law enforcement from the fact that Binance itself was still substantially operating in the United States market and dependent on U.S.- based market makers for daily trading liquidity without registering with FinCEN or complying with the Bank Secrecy Act's anti-money laundering requirements, in violation of 18 U.S.C. § 1960(a) and the Bank Secrecy Act.

103. Incredibly, Binance and Zhao lied to and manipulated their own outside counsel, including partners at some of America's most prestigious law firms, regarding Binance's operations in the United States. This caused Binance's outside counsel, including highly respected practitioners, to unwittingly misrepresent to Article III judges that Binance was a completely foreign exchange with no U.S. operations whatsoever. Binance and Zhao used these judicial misrepresentations to evade the jurisdiction of United States courts. For example, in a civil complaint filed in the United States District Court for the Southern District of Florida pursuant to the diversity jurisdiction statute, Binance and Zhao caused its outside counsel, including a former federal prosecutor and a seasoned Supreme Court practitioner, to misrepresent to the district court in a motion to dismiss for lack of personal jurisdiction that "Binance.com . . . is not a cryptocurrency exchange for United States users—indeed, United States users are restricted from use of Binance.com." The factual admissions in Binance's and Zhao's criminal pleas have revealed and completely unraveled this lie, and so the jig is now up. As the Second Circuit Court of Appeals found just last month, Binance in fact "has a substantial presence" in the United States, "with servers, employees, and customers throughout the country." And as the United States put it in the sentencing memorandum it filed on April 23, 2024 in Zhao's criminal prosecution, Zhao and Binance "violated U.S. law on an unprecedented scale" and "massively profited from the U.S. financial system, U.S. businesses, and U.S. customers—

all without playing by U.S. rules" and "with deliberate disregard for the company's legal responsibilities and for its capacity to cause significant harm".

104. In its November 2023 criminal plea, Binance admitted that its conduct as set forth above constituted a conspiracy to violate the Bank Secrecy Act's anti-money laundering requirements and 18 U.S.C. § 1960(a)'s prohibition on operating an unregistered money transmitting business. Binance's plea to violating 18 U.S.C. § 1960(a) is necessarily an admission that every financial transaction that it conducted on the Binance.com exchange (i.e., all of the financial transactions that occurred on the Binance.com exchange) were violations of 18 U.S.C. § 1956(a)(1)(A)(i) by virtue of 18 U.S.C. § 1956(c)(7)(A)'s cross-reference to 18 U.S.C. § 1961(1).

105. The Commodity Futures Trading Commission ("CFTC") has also filed a complaint against Zhao and Binance in the Northern District of Illinois. See Dkt. 23-CV-01887. In the complaint, the CFTC alleged as follows as relevant here, making it clear that Binance's business model was predicated on money laundering and targeting U.S.-based customers to use the exchange:

a. Binance, under Zhao's direction, operating an exchange for trading commodities such as Bitcoin and Ethereum for persons in the United States since at least 2019. Dkt. 1 ¶2. 20-30% of Binance's traffic "comes from the US." ¶107.

b. Binance strategically targeting United States customers despite publicly pledging to block such customers. ¶3. Binance and Zhao also knew that doing so subjected them to U.S. law and regulations. *Id.*

c. Binance and Zhao facilitated violation of U.S. law by instructing customers in the United States to use virtual private networks to obscure their

locations, allowed customers who had not submitted proof of identity to use their platform, and directed U.S. businesses and customers to incorporate shell companies to evade Binance's own compliance controls. ¶7.

d. Despite restricting access to its platform from certain jurisdictions beginning in mid-2019, Binance left open a "loophole" for customers to "sign up, deposit assets, trade, and make withdrawals without submitting to any KYC procedures as long as the customer withdrew the value of two BTC (Bitcoin) in one day. Two Bitcoin are currently worth approximately $120,000. ¶92. It was Zhao personally who implemented this policy. Id. Zhao personally demanded that Binance *not* implement KYC on Binance.com.¶100. And Zhao believed that if Binance's compliance controls were "too stringent" no one would use the exchange. *Id.*

e. Binance knowingly financed transactions from Hamas and senior Binance officials acknowledged with respect to other known criminals: "Like come on. They are here for crime" …. "we see the bad, but we close 2 eyes." ¶104. Binance intentionally tolerated customers using the Binance platform for illegal activity. ¶105.

f. Senior Binance officials even instructed "very closely associated with illicit activity" to open a new Binance account in order to "continue trading on the platform," which was "consistent with Zhao's business strategy." ¶106.

106. In sum, the Defendants' knowing and willful conduct so egregiously and systematically assisted fraud syndicates that, in addition to constituting the RICO predicate offenses to which Binance pled guilty and to which Zhao essentially admitted in his own criminal plea, it also constituted aiding and abetting of the wire frauds that syndicates were committing against United States citizens as well as the money laundering that those

syndicates had to commit in order to successfully complete their wire frauds.

E. The Plaintiffs' Victimization and Economic Injuries

a. Plaintiff Lenny Licht

107. In June 2021, Plaintiff Lenny Licht ("Lenny") received a Facebook friend request from a supposed woman named Tina Ling. According to her Facebook profile, "Tina Ling" was Facebook friends with one of Lenny's high school classmates. Licht's Facebook profile conspicuously identified his location as Plano, Texas. Ling's apparent common connection to Lenny's high school classmate convinced Lenny to accept Tina Ling's friend request, and Tina soon thereafter began communicating with Lenny via Facebook Messenger and WhatsApp. Tina used Lenny's phone number, which had an area code associated with Dallas, to communicate with Lenny via WhatsApp. At first, it was just friendly banter, which included Lenny discussing his life in the Dallas area. Within about a month, however, Tina Ling turned the conversation to cryptocurrency investing. Lenny had no experience with cryptocurrency, but Tina Ling convinced Lenny that he should invest his money in a supposedly successful crypto mining operation called LuxKey, which would provide both safety and positive returns.

108. Lenny, a 75-year-old widower who had lost his wife to pancreatic cancer only a few years before, fell for "Tina Ling's" false representations. Over several months, at the instruction of "Tina Ling," Lenny purchased over $2.7 million of USDT on the regulated, U.S.-based cryptocurrency exchanges Coinbase.com and Crypto.com. This represented almost the entirety of Lenny's life savings. Also at "Tina Ling's" instruction, Lenny transferred all of this USDT to a pair of self-custodied wallets that he understood to be LuxKey. The transfers were done in approximately a dozen installment transactions that occurred over a period of months.

109. LuxKey, of course, was not a cryptocurrency mining operation. It was not an

investment at all. Indeed, "LuxKey" did not exist. The wallets to which Lenny transferred his cryptocurrency were simply self-custodied digital wallets controlled by the criminal syndicate for which "Tina Ling" was simply a fictitious front. In short, it was a scam.

110. Between approximately August 2021 and June 2022, an individual representing himself as a LuxKey customer support specialist sent repeated messages to Lenny via WhatsApp (using Lenny's Dallas-based phone number) regarding the status of Lenny's "LuxKey investment." The supposed LuxKey customer support specialist also sent group messages, via WhatsApp, to Lenny and the person representing herself as "Tina Ling" regarding Lenny's "investment." These communications included numerous false statements regarding the returns that Lenny had earned on the investment and the need for Lenny to make additional payments to LuxKey to keep his investment from becoming inactive.

111. In July 2022, "Tina Ling" and "LuxKey" suddenly disappeared. Finally realizing that he had been defrauded of almost his entire life savings, Lenny contacted law enforcement and retained a private blockchain investigative agency called CipherBlade to track, trace, and recover the stolen cryptocurrency. According to CipherBlade's website, it has worked with law enforcement to recover millions of dollars in stolen cryptocurrency.

112. USDT is built on the Ethereum blockchain. Using a software program called Chainanalysis Reactor, which is used by law enforcement agencies including the FBI and the Secret Service, CipherBlade's forensic experts were able to track and trace the cryptocurrency that Lenny had sent to "LuxKey." Those self-custodied wallets then transferred Lenny's USDT to intermediary self-custodied wallets (*i.e.*, not to exchanges) that the criminal syndicate controlled; those intermediary self-custodied wallets then transferred the USDT to nine Binance.com exchange accounts that Binance allowed the scammers to open and utilize

unfettered for transactions that bore all the obvious hallmarks of money laundering illicit funds. Unfortunately, CipherBlade concluded that the fraud syndicate was successful in using Binance as a cash-out point, meaning that Binance allowed the syndicate to launder the USDT that it stole from Lenny and convert it into fiat currency that is untraceable and unrecoverable.

113. Each of the nine Binance accounts to which the fraud syndicate transferred the stolen USDT is associated with a unique identification address comprising more than 40 characters. The fraud syndicate's laundering of illicit funds through these nine Binance wallets began no later than August 2021. CipherBlade's analysis concluded that between August 2021 and November 2022, these nine Binance accounts received over $40 million of USDT across approximately 140 transactions, traceable to the two "LuxKey" self-custodied wallets to which Lenny had transferred his USDT. The vast majority of the transfers (more than $34 million worth of USDT) occurred between August 2021 and July 2022, allowing for a reasonable inference that the entirety of Lenny's USDT was laundered on the Binance.com exchange. All of these money laundering transfers, including the addresses associated with the nine Binance accounts, are identified in Exhibit A appended to this complaint. CipherBlade's findings indicate that the LuxKey fraud was extensive, prolonged, involved victims other than Lenny, and involved transfers from self-custodied wallets to the Binance.com exchange that had all the obviously hallmarks of money laundering.

114. The CipherBlade findings allow for a reasonable inference that all of the USDT stolen from Lenny was laundered on the Binance.com exchange. The nine Binance.com accounts to which the fraud syndicate transferred Lenny's stolen USDT are no longer active, and further investigation confirmed that the wallets are essentially empty, which means the syndicate was able to successfully use those Binance wallets as cash-out points, converting the USDT to

fiat currency and leaving Lenny without any means of recovering the specific USDT assets that were stolen from him.

b. Plaintiff Zhengjun Cai

115. On or about November 28, 2021, Plaintiff Zhengjun Cai ("Cai") met a man in a group chat on WeChat, a social messaging application. Cai specified on her account that she was a realtor in California. The man contacted Cai initially under the pretext of seeking her help to buy a property, suggesting that he read her profile and was aware that she lived and worked in the United States.

116. The man eventually told Cai about his alleged investment in a pool that had earned him significant returns on his crypto funds. He encouraged Cai to participate.

117. On or about December 2, 2021, Cai agreed to join the pool and invest crypto funds from her self-custodial wallet. Unbeknownst to her, when she paid the nominal fee that she believed was a prerequisite to participate in pool, she was actually executing malicious code on her self-custodied wallet that gave the scammer unfettered access to all the funds in her wallet.

118. Between December 2, 2021 and February 14, 2022, Cai made seven deposits of USDT into her self-custodied wallet. After Cai made her initial deposit of USDT into her self-custodied wallet, it appeared that her assets were secure and that she was earning profits on her investment.

119. However, three unauthorized withdrawals of cryptocurrency were made from Cai's self-custodied wallet on February 3, February 7, and February 14, 2022. These fraudulent withdrawals were made without her knowledge or consent.

120. Cai's losses incurred as a result of the pig butchering scheme total $741,170.21 USDT. Cai's stolen assets comprised her life savings and funds she had set aside to refinance her

home in hopes of a better life after retirement.

121. Through investigation on the public blockchain website etherscan.io, Cai has been able to verify that a substantial portion of her stolen assets were laundered through the Binance.com exchange.

c. Plaintiff Daniel Chang

122. On or about December 14, 2021, Daniel Chang ("Chang") was contacted by a woman on WeChat. Chang's WeChat profile lists his region as San Jose, California, suggesting the woman was aware that he lived in the United States.

123. Chang and this woman began chatting and became very friendly. The woman then introduced Chang to an investment opportunity that she claimed would pay "high interest."

124. Chang was interested in the opportunity but sought additional information about how the investment worked. The woman explained the process and convinced Chang to join and deposit USDT into his self-custodied wallet.

125. On December 14, 2021, Chang unknowingly executed a malicious code on his wallet which enabled defrauders to access the entire wallet and make withdrawals without his consent. This code was likely disguised as an entry fee that Chang had to pay in order to participate in the investment.

126. On or about December 14, 2021, Chang began making deposits of small amounts of USDT into the investment. Over the next several weeks, Chang made four deposits of USDT into his self-custodied wallet in order to fund the investment.

127. Initially, the investment operated in accordance with the woman's description and Chang believed he would be able to make a return on his investment. Based on this observation, Chang continued depositing USDT into his self-custodied wallet and making larger deposits over

time.

128. Between January 16, 2022 and March 11, 2022, however, Chang had a total of $289,916 USDT stolen from his self-custodied wallet in a series of unauthorized withdrawals. The withdrawals were done without his knowledge or consent.

129. Through investigation on the public blockchain website etherscan.io, Chang has been able to verify that a substantial portion of his stolen assets were laundered through the Binance.com exchange.

d. Plaintiff Henry Chen

130. On or about January 17, 2022, a person going by the name Jenny, who allegedly lived in Richmond, CA, contacted Plaintiff Henry Chen ("Chen") on Hinge. Chen's profile on Hinge reflected that he was located in San Francisco, CA, and Chen wrote Jenny early on that he was born and raised and went to college in the State of California.

131. After befriending Chen, Jenny informed Chen that she was earning significant income investing cryptocurrency.

132. Having lured Chen in with the prospect of similar income, Jenny directed Chen to download an application for a self-custodied wallet and open the link for the investment platform using the application's browser. Chen did as he was instructed.

133. Once on the investment platform's website, Jenny directed Chen to make a purchase that would allow him to participate in the investment. Chen did as he was instructed, and this action most likely executed malicious code on his self-custodied wallet, granting scammers working with Jennie direct access to all the USDT in his self-custodied wallet.

134. Chen deposited a total of $121,516 USDT into his self-custodied wallet as part of the investment.

135. Between January 2022 and March 2022, scammers withdrew all the USDT from Chen's self-custodied wallet. The withdrawals were done without Chen's knowledge or consent.

136. Through investigation on the public blockchain website etherscan.io, Mr. Chang has been able to verify that a substantial portion of his stolen assets were laundered through the Binance.com exchange.

e. Plaintiff Dominic Chow

137. On or about January 19, 2022, Plaintiff Dominic Chow ("Chow") met an individual named Eileen Chou on WhatsApp. Chow's WhatsApp was linked to a U.S. phone number with a Massachusetts-area area code, which is where Chow lives. Chow also wrote to Eileen at one point that he lived in Los Angeles.

138. Chou told Chow about an investment opportunity for cryptocurrency using a particular self-custodied wallet.

139. After about 2 months, Chow decided to participate in the investment. Eileen directed Chow to purchase a voucher using his self-custodied wallet in order to participate in the investment, which Chow did on March 8, 2022.

140. Unbeknownst to Chow, he was actually executing a malicious code on his wallet that gave scammers working with Eileen perpetual and unlimited access to withdraw all the USDT in his account.

141. Between March 8, 2022 and March 18, 2022, Chow deposited a total of $280,914 USDT into his self-custodied wallet to participate in the liquidity mining pool.

142. Scammers withdrew all these funds from his self-custodied wallet without his knowledge or consent.

143. Through investigation on the public blockchain website etherscan.io, Chow was

able to verify that a substantial portion of his stolen assets has been laundered through the Binance.com exchange.

144. Chow promptly reached out to Binance for assistance in freezing the wallets and recovering his funds. Binance responded that the wallet(s) belonged to "SafePal," a "Binance Broker," with many users whose identities are unknown to it.

145. Binance told Chow that Binance "was not responsible for the management of the assets on the broker's wallet so [it was] unable to help [Chow] track the funds further."

f. Plaintiff Chengguo Dong

146. On or about October 26, 2021, Plaintiff Chengguo Dong ("Dong") received a text message on his phone number with U.S. country code from an individual who claimed to have messaged the wrong number. The conversation eventually moved to Line, a social media application which was also linked to Dong's U.S phone number.

147. The individual extended Dong an investigation to participate in an investment opportunity using funds from his self-custodied wallet.

148. On or about October 27, 2021, Dong purchased a voucher using funds in his self-custodied wallet in order to start investing. Dong had no idea that, by purchasing the voucher, he had executed malicious code on his wallet that allowed third parties to withdraw all the USDT in his self-custodied wallet.

149. Between October 29, 2021 and November 12, 2021, Dong made several deposits of USDT into his self-custodied wallet in order to participate in the investment. These funds comprised his life savings.

150. On November 12, 2021, fraudsters drained Dong's entire self-custodied wallet, leaving him with nothing. Dong, a 50-year-old Chinese immigrant residing in Burlingame,

California, had been planning to use the funds to purchase a home for his family, as well as pay his daughter's educational expenses.

151. Through investigation on the public blockchain website etherscan.io, Dong has been able to verify that a substantial portion of his stolen assets were laundered through the Binance.com exchange.

g. Plaintiff Ihab William Francis

152. On or about September 18, 2021, Plaintiff Ihab William Francis ("Francis") was contacted by an individual on LinkedIn. Francis' LinkedIn profile displays his location as the New York Metropolitan area.

153. After asking Francis where he lived and what he did for a living, the individual mentioned that he was a cryptocurrency investor and offered to explain to Francis how he had successfully made money in the cryptocurrency market. The individual offered Francis a "time-limited opportunity" to earn interest in an investment pool using cryptocurrency in a self-custodied wallet.

154. As part of the fraudulent pool scheme, Francis was directed to "join the node" and receive a voucher into his self-custodied wallet in order to join the pool. Francis did as he was instructed, and in the process unknowingly executed malicious code that permitted third-party scammers to withdraw all the USDT in his self-custodied wallet.

155. After joining the pool through, Francis made small transfers to the pool from his self-custodied wallet on November 3 and 8, 2021. The initial contributions appeared to be yielding interest in accordance with Francis's understanding, so he continued to make contributions.

156. Francis made 12 deposits of USDT into his self-custodied wallet between

November 3, 2021 and January 10, 2022.

157. Francis had all the funds in his self-custodied wallet withdrawn without his knowledge or consent in a series of four swipes. All told, Francis had $462,883.48 USDT stolen.

158. The losses incurred by Francis as a result of the scheme included assets that Francis had withdrawn from his 401K, Roth IRAs, and family's personal savings accounts. Francis was left without any savings or retirement funds, leaving him and his family in financial ruin.

159. Through investigation on the public blockchain website etherscan.io, Francis has been able to verify that a substantial portion of his stolen crypto assets were laundered through the Binance.com exchange.

h. Plaintiff John Gordon

160. On or about June 1, 2022, Plaintiff John Gordon matched on Hinge with a person going by the name "Laura", who allegedly lived in New York. Gordon's profile on Hinge indicated he was based in a city in the United States and was matched to other profiles based in part on proximity to his location.

161. After befriending Gordon, Laura informed him about her interest in cryptocurrency and her successful investment in cryptocurrency using a self-custodied wallet.

162. Having lured Gordon in with the prospect of similar income, Laura directed Gordon to access the investment platform using his self-custodied wallet. Gordon did as he was instructed, not realizing that at one point he executed malicious code that gave scammers unlimited and perpetual access to the funds in his self-custodied wallet.

163. On or about June 10, 2022, Gordon began making small deposits into his self-custodied wallet to test the investment platform.

164. After the initial deposits earned the promised interest on his original investment, Gordon continued to make additional deposits. Between June 10 and June 23, 2022, Gordon made 8 deposits of USDT into his self-custodied wallet in an amount totaling approximately $625,000.

165. All the USDT in Gordon's self-custodied wallet was then fraudulently withdrawn in unauthorized transactions.

166. Gordon lost his life savings and other funds needed to support his dependent father.

167. Through investigation on the public blockchain website etherscan.io, Gordon has been able to verify that a substantial portion of his stolen assets were laundered through the Binance.com exchange.

i. Plaintiff Dalton Green

168. On or about December 4, 2021, Plaintiff Dalton Green ("Green") heard about an investment opportunity that was earning significant income from one of his friends who, like he, was based in Colorado. The scammer behind the fraud had convinced Green's friend, whom the scammer knew was based in Colorado, to recruit other friends to participate in what he believed at the time was a legitimate investment pool. Green was one of the individuals that was recruited.

169. Green accessed the platform using his self-custodied wallet. Green used funds from his self-custodied wallet to purchase a voucher that would allow him to join the pool. This action most likely executed malicious code that gave third parties access to all the USDT in his wallet.

170. To fund the pool, Green deposited a total of $71,096 USDT into his self-custodied

wallet.

171. In December 2021, scammers withdrew all the USDT from his self-custodied wallet. The withdrawal was done without Green's knowledge or consent.

172. Green's life has been devastated both financially and emotionally. The financial loss caused a great deal of stress to, and ultimately ended, his marriage, triggering a spiraling depression.

173. Through investigation on the public blockchain website etherscan.io, Green has been able to verify that a substantial portion of his stolen assets were laundered through the Binance.com exchange.

j. Plaintiff Michael Grilli

174. On or around November 11, 2021, Plaintiff Michael Grilli met a woman through a dating website. Grilli's profile on the site indicated that he was based in Florida and his settings were configured to facilitate him meeting people locally. The woman told Grilli she lived in the same area as him in Florida.

175. After befriending Grilli, the woman encouraged him to join a cryptocurrency investment pool from which she insisted Grilli would be able to earn significant income.

176. The woman directed Grilli to deposit USDT into his self-custodied wallet and open the link for the pool from his wallet's browser.

177. Unbeknownst to Grilli, by following the woman's instructions, he provided scammers the ability to execute malicious code on his wallet, which then allowed the scammers to withdraw all of the USDT from his self-custodied wallet without his authorization or consent.

178. Between December 2021 to March 2022, scammers, through unauthorized transactions, stole all of the USDT Grilli deposited in his self-custodied wallet, amounting to

approximately $3,718,480.

179. The financial loss has devastated Grilli. Grilli, age 83, saw his savings depleted and had taken out multiple loans to fund his self-custodied wallet. As a result of his grave financial loss, he has suffered significant mental and emotional distress and anxiety.

180. Through investigation on the public blockchain website etherscan.io, Grilli has been able to verify that a substantial portion of his stolen assets were laundered through the Binance.com exchange.

k. Plaintiff Iraklis Karabassis

181. In or around January 2022, Plaintiff Iraklis Karabassis met a woman going by the named Zhu Bella Hannah Ziaohan Zhu ("Hannah") on Instagram. The two eventually began to communicate on WhatsApp using Karabassis's phone number with a U.S. country code and Florida area code. After Karabassis mentioned that he was based in South Florida, Hannah told him that she would make plans to visit him the United States within the next two months.

182. Through subsequent correspondence and phone calls, Hannah presented Karabassis with the opportunity to invest in a very lucrative cryptocurrency investment pool using a digital crypto wallet. Hannah instructed Karabassis to download the required self-custodied wallet application and then transfer crypto into his account.

183. Under the guise of giving Karabassis access to the pool, Hannah sent him a voucher to through which he would receive a nominal amount of crypto into his self-custodied wallet. Karabassis did as Hannah instructed and accepted the voucher, unwittingly executing malicious code on his wallet that would allow the scammers working with Hannah unfettered access to all the USDT in his self-custodied wallet.

184. Over the next several weeks, Karabassis transferred $1,180,760 USDT into his

self-custodied wallet to participate in the pool.

185. On March 4, 2022, scammers transferred $1,180,760 USDT out of Karabassis's self-custodied wallet without his knowledge or consent.

186. A month later, Karabassis deposited another $4,899 USDT into his digital believing that this would allow him to regain access to his $1,180,760 USDT and to the interest that it had allegedly accrued. The scammers subsequently withdrew that amount from his wallet as well.

187. Through investigation on the public blockchain website etherscan.io, Karabassis has been able to verify that a substantial portion of his stolen assets, proceeds of the crime, were laundered through the Binance.com exchange.

l. Plaintiff Nader Lobandi

188. On or around March of 2022, a person going by the name of Aimee contacted Plaintiff Nader Lobandi ("Lobandi") through a dating website. Their conversation moved to WhatsApp, where Lobandi used a phone number with U.S. country code and a Massachusetts area code.

189. After befriending Lobandi, Aimee encouraged him to join a cryptocurrency investment pool from which she insisted he would be able to earn significant income. She directed Lobandi to deposit USDT into his self-custodied wallet to contribute to the pool.

190. Aimee then directed Lobandi to open a link that she provided him in his self-custodied wallet browser. Aimee directed him to click a button to "join the node" and start participating in the pool. Unbeknownst to Lobandi, this action allowed scammers to access and initiate transfers from his self-custodied wallet without his knowledge or consent.

191. On or around April 12, 2022, scammers, through unauthorized transactions, stole

all of the USDT from Lobandi's self-custodied wallet, amounting to approximately $92,640 USDT. These withdrawals were done without Lobandi's knowledge or consent.

192. Lobandi lost a significant portion of his life savings and suffered emotional and mental distress as a result of these unauthorized transactions. Due to the mental distress Lobandi experienced soon after the incident, he was hospitalized for two weeks for severe anxiety and depression.

193. Through investigation on the public blockchain website etherscan.io, Lobandi has been able to verify that a substantial portion of his stolen assets were laundered through the Binance.com exchange.

m. Plaintiff James Moskwa

194. On or around October 10, 2021, Plaintiff James Moskwa ("Moskwa") was introduced to a woman named "Tresa" on Instagram. Moskwa's profile was public with many of his posts tagged with a Rhode Island location. Moskwa also informed "Tresa" that he lived in Rhode Island and start of their conversation.

195. Over several weeks, Moskwa began to develop a friendship with Tresa. Moskwa and Tresa spoke often, and she eventually brought up the topic of crypto investments. Tresa told Moskwa that her uncle was assisting her in making investments. She told Moskwa that her uncle was a broker involved in a cryptocurrency investment opportunity. Tresa convinced Moskwa to obtain the required self-custodied wallet and participate in the investment pool as well. She eventually introduced Moskwa to her uncle to have him describe the technicalities of the pool.

196. On or around November 1, 2021, Moskwa obtained his self-custodied wallet, and Tresa walked Moskwa through the process of purchasing the needed entry voucher on the wallet application. Moskwa purchased the voucher using cryptocurrency that Tresa sent him.

197. Unbeknownst to him, by accepting cryptocurrency from Tresa, Moskwa actually had executed malicious code on his wallet, allowing scammers working with Tresa access to all the USDT in his wallet.

198. On or about November 16, 2021, Moskwa started depositing USDT into his self-custodied wallet. Between November 16, 2021 and January 21, 2022, Moskwa made six deposits into his self-custodied wallet to participate in the pool. 161. Between December 24, 2021 through January 21, 2022, scammers withdrew all the USDT from Moskwa's self-custodied wallet.

199. Shortly after the unauthorized withdrawals, Moskwa contacted the pool's supposed customer service department to inform the pool of the fraudulent withdrawals. The customer service agent informed Moskwa that his account was temporarily frozen and that he would have to deposit an additional $262,798.00 for "account risk verification" to unfreeze his account and access his assets.

200. Fearful of losing the hundreds of thousands of dollars he already had deposited, Moskwa agreed to comply with the request and continued to make additional deposits of USDT. These funds were also withdrawn from his self-custodied wallet without his knowledge or consent.

201. All told, Moskwa lost $1,417,654.06 USD because of the fraudulent withdrawals. These funds comprised his life savings, retirement fund, and even some personal loans from friends. As a result of the scam, Moskwa had to refinance his mortgage and incurred substantial tax penalties from premature withdrawals from his retirement accounts. The substantial financial loss has caused him significant emotional distress.

202. Through investigation on the public blockchain website etherscan.io, Moskwa has

been able to verify that a substantial portion of his stolen assets were laundered through the Binance.com exchange.

n. Plaintiff Anh Nguyen

203. On or about October 16, 2021, Plaintiff Anh Nguyen ("Nguyen") was contacted by a woman named "Teyana Cuffe" on Facebook. Nguyen's profile had his location listed as Anaheim, CA and Nguyen told her during their conversation that he was located in California.

204. After befriending Nguyen, this individual informed him of a cryptocurrency investment opportunity using a self-custodied wallet.

205. Having convinced Nguyen that he could gain significant returns on USDT investments through the investment pool, Teyana directed Nguyen to open a link to the platform he was sent and purchase a voucher to start investing. Nguyen was instructed that he had to deposit USDT into his self-custodied wallet to collect interest through the pool.

206. On or about October 29, 2021, Nguyen did as he was instructed and purchased a voucher. Unbeknownst to Nguyen, he had executed malicious code that allowed scammers direct, unlimited, and indefinite access to funds in his self-custodied wallet.

207. Initially, the pool operated as described and Nguyen appeared to earn interest on his deposited USDT.

208. However, on or about October 29, 2021, all the USDT was removed from Nguyen's self-custodied wallet by scammers. When Nguyen inquired to the pool's supposed customer service department about the withdrawal, he was told that his assets had been contributed to a "special pool" in order to yield higher earnings and that all of his funds were still in his self-custodied wallet.

209. Nguyen was also informed that he needed to contribute another $200,000 USDT

into his self-custodied wallet in order to regain access to his assets and earn his reward. On or about November 18, 2021, Nguyen deposited additional USDT into his wallet to meet the $200,000 USDT threshold requirement.

210. Immediately after his wallet reached $200,000 USDT, the scammers drained his self-custodied wallet again. All told, Nguyen lost a total of $222,946 USDT because of the fraudulent transactions.

211. The financial and emotional results of the loss have been devastating for Nguyen and his family, causing significant mental anguish and suicidal thoughts. Nguyen and his wife have lost the majority of their life savings and are struggling to make ends meet.

212. Through investigation on the public blockchain website etherscan.io, Nguyen has been able to verify that a significant portion of his stolen assets were laundered through the Binance.com exchange.

o. Plaintiff Brian Rothaus

213. On or around April 11, 2022, a woman contacted Plaintiff Brian Rothaus ("Rothaus") through Facebook under the guise of seeking golf advice from Rothaus, who is an avid golfer. Rothaus's Facebook page included photographs and postings that made it obvious that he resides in Pennsylvania. After chatting with Rothaus about golf, the woman told Rothaus about her investments in cryptocurrency and asked Rothaus to participate in an investment pool. The woman directed Rothaus to obtain the necessary self-custodied wallet and to deposit USDT into the wallet. The woman told Rothaus that he could easily transfer the funds from his self-custodied wallet to his personal account.

214. The woman then directed Rothaus to open the link for the pool in his self-custodied wallet browser.

215. Rothaus made one deposit of 247,456.34 USDT into his self-custodied wallet on or around October 26, 2022. On or around October 27, 2022, Rothaus clicked a button to "receive" a node and participate in the pool, which unknowingly executed malicious code on his self-custodied wallet giving scammers direct and unlimited access to his account.

216. Later that same day, scammers stole all of the USDT in Rothaus's self-custodied wallet totaling approximately $247,456 USDT. This withdrawal was done without his knowledge or consent.

217. Rothaus lost his IRA savings as a result of this scam and suffered substantial emotional and mental distress due to the financial loss.

218. Through investigation on the public blockchain website etherscan.io, Rothaus has been able to verify that a substantial portion of his stolen assets were laundered through the Binance.com exchange.

p. Plaintiff Gordon Shaylor

219. On or around December 17, 2021, Plaintiff Gordan Shaylor ("Shaylor") was contacted by a woman named Sa Li through Facebook. Shaylor's public Facebook profile displayed that he lived in South Florida.

220. After befriending Shaylor, Sa Li began communicating with him on WhatsApp and encouraged Shaylor to join a cryptocurrency investment pool, which she assured Shaylor was a safe investment opportunity.

221. To join the pool, Sa Li directed Shaylor to obtain a self-custodied wallet using a specific application and deposit USDT into the wallet.

222. Shaylor was then instructed to open the link for the pool through the wallet application's browser. Shaylor was instructed to purchase a "node," which unbeknownst to him

executed malicious code on his self-custodied wallet and provided scammers unfettered access to the wallet.

223. To fund the supposed pool, Shaylor made multiple deposits of USDT into his self-custodied wallet over the course of nine months. The pool then fraudulently reported to Shaylor that he was earning significant interest on his deposits, which convinced Shaylor to heed Sa Li's advice to continue to deposit more and more money into his self-custodied wallet. In truth, Sa Li was simply a fictious name under which scammers were operating.

224. On or around August 2022, the scammers stole all of the USDT in Shaylor's self-custodied wallet, amounting to approximately $1,200,000. The fraudulent withdrawal was done without Shaylor's permission or consent.

225. As a result of the fraud scam, Shaylor lost all of his life savings at age 60 and has incurred substantial debt from loans taken during the process. He also experienced significant anxiety and emotional distress due to the financial loss.

226. Shaylor subsequently retained the services of forensic crypto tracers who concluded with "very strong confidence" that the scammers utilized the Binance.com exchange to launder the assets they stole from Shaylor.

q. Plaintiff Richard Slavant

227. On or about September 27, 2021, a woman contacted Plaintiff Richard Slavant ("Slavant") on WhatsApp. Slavant's phone number on WhatsApp had a United States country code and an area code from Louisiana. The woman claimed she had messaged the wrong number.

228. After befriending Slavant, the woman informed him that she was earning significant income on her cryptocurrency by participating in an investment pool.

229. Having lured Slavant in with the prospect of similar income, the woman directed Slavant to download an application and obtain a self-custodied wallet. She then instructed him to open a link using the self-custodied wallet application's browser. Slavant complied, not realizing that the supposed investment pool was simply a fraud.

230. Once on the fraudulent pool's site, the woman directed Slavant to purchase a node that would allow him to join the pool. On or about October 8, 2021, Slavant did as he was instructed and unknowingly executed malicious code that gave scammers direct and unfettered access to all the USDT in his self-custodied wallet.

231. Between October 9 and November 9, 2021, Slavant made four deposits of USDT into his self-custodied wallet to fund the pool.

232. On or about November 13, 2021, scammers withdrew all the USDT from Slavant's self-custodied wallet. The fraudulent withdrawal was done without Slavant's knowledge or consent.

233. As a result of the scam, Slavant lost approximately $52,349.87 USDT, comprised of funds from loans and other personal savings. The scam has been devastating to Slavant, both financially and emotionally, and resulted in significant distress.

234. Through investigation on the public blockchain website etherscan.io, Rothaus been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchage.

r. Plaintiff Nathanial Thrailkill

235. On or about December 4, 2021, after hearing about an investment opportunity from a friend based in the United States that was earning significant income from his friends, Plaintiff Nathanial Thrailkill ("Thrailkill") decided to join what they all thought was a

cryptocurrency investment pool.

236. Thrailkill accessed the platform for the supposed pool using the application for his self-custodied wallet on both his phone and desktop.

237. Between December 7, 2021 and December 8, 2021, Thrailkill made 3 deposits totaling approximately $100,308 USDT to fund the pool.

238. Once Thrailkill's money was deposited into his wallet, he was told to accept a voucher in order to pay the "mining fee" so that he could begin "investing." Unbeknownst to Thrailkill, by accepting the voucher, he executed malicious code that allowed scammers to gain access to and withdraw his USDT.

239. On December 10, 2021, mere hours after making his last deposit, scammers stole all the USDT in Thrailkill's self-custodied wallet. The fraudulent withdrawal was done without Thrailkill's knowledge or consent.

240. Thrailkill lost his entire life savings, resulting in significant emotional and mental distress.

241. Through investigation on the public blockchain website etherscan.io, Thraikill has been able to verify that a substantial portion of his stolen assets were laundered through the Binance.com exchange.

s. Plaintiff Jack Yao

242. On or around May 30, 2022, Plaintiff Jack Yao ("Yao") was introduced to a cryptocurrency investment pool opportunity by his friend, Tao Wang ("Wang"), who also lived in San Diego, CA, who had been contacted by a woman named Li Zhu on WeChat. The woman was aware that both Yao and Wang were U.S. residents, as she sent Tao photos of her that were purportedly taken at a shopping mall in San Diego.

243. After communicating with Wang about the investment pool, Yao agreed to join the pool as well. Unfortunately, both Wang and Yao were victims of a fraud.

244. On or around May 30, 2022, Yao deposited USDT into his self-custodied wallet and opened the provided link for the pool's platform through the browser on his self-custodied wallet application.

245. To fund the pool, Yao made 6 deposits of USDT into his self-custodied wallet.

246. On or around June 29, 2022, scammers drained Yao's self-custodied wallet of all the USDT that he had deposited into it. Yao promptly contacted Wang, who informed him that his wallet had also been drained. Yao immediately contacted the pool's supposed customer service department about the unauthorized withdrawal, and he was informed that his account had been "frozen" and that his USDT had been "transferred to a custodian account because they detected abnormal activit[y]."

247. The supposed customer service representative then instructed Yao that he would have to deposit additional funds into his self-custodied wallet in order to unfreeze his account. On or around July 7, 2022, Yao, desperate to retrieve his crypto, complied with the demand and deposited additional funds into his self-custodied wallet. Hours later, Yao's self-custodied wallet was drained again.

248. Scammers, through unauthorized transactions on June 29 and July 9, 2022, had stolen all of the USDT in Yao's self-custodied wallet, totaling $310,000 USDT. These withdrawals were done without his knowledge or consent.

249. Yao has lost his entire life savings and suffered significant mental and emotional distress as a result of the unauthorized transactions.

250. Through a forensic blockchain investigation conducted by the firm CoinStructive,

Yao was able to determine that a substantial portion of his stolen assets were laundered through the Binance.com exchange.

t. Plaintiff Jun Zhai

251. On or about February 23, 2022, a person going by the name "Julie", who supposedly lived in Seattle, contacted Plaintiff Jun Zhai ("Zhai") on WeChat. Zhai's WeChat profile was set to Seattle, Washington and Julie's profile appeared among those labeled as "People Nearby."

252. Julie told Zhai that she was in the cosmetic surgery industry and was visiting San Diego, California on a business trip. After befriending Zhai, Julie told him about her hobbies and informed Zhai that she was earning significant income participating in a cryptocurrency investment pool.

253. Zhai believed the pool was legitimate and agreed to participate. Julie directed Zhai to download a self-custodied wallet application and to open the link for the pool using the self-custodied wallet's browser.

254. On or about February 28, 2022, Zhai did as he was instructed and purchased a voucher to begin transferring funds into his self-custodied wallet. In the process, he unsuspectingly executed malicious code on his wallet that gave scammers unfettered and unlimited access to the assets in his self-custodied wallet.

255. Between March 2 and March 22, 2022, Zhai made four deposits of $69,747 USDT into his self-custodied wallet to fund the pool.

256. On or about April 5, 2022, scammers withdrew all the USDT from Zhai's self-custodied wallet. The withdrawal was done without Zhai's knowledge or consent.

257. Zhai lost his entire retirement fund and life savings as a result of the scam. The

scam led Zhai to be depressed and negatively impacted his job performance.

258. Through investigation on the public blockchain website etherscan.io, Zhai has been able to verify that a substantial portion of his stolen assets were laundered through the Binance.com exchange.

V. THE DEFENDENTS' CIVIL RICO LIABILITY FOR THE PLAINTIFFS' ECONOMIC INJURIES

A. The RICO Enterprises

259. Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 258 above.

260. The facts alleged in this complaint establish at least four association-in-fact RICO enterprises and one corporate RICO enterprise (Binance), which are described as follows:

Enterprise #1 (Association-in Fact Enterprise)

261. Binance and BAM constituted an association-in-fact RICO enterprise, the common purposes of which were (i) to allow Binance to operate as an unlicensed money transmitting business, in violation of 18 U.S.C. § 1960(a); (ii) to allow Binance to facilitate and conduct transactions on the Binance.com exchange that the Defendants knew involved illicit proceeds of criminal offenses, in violation of 18 U.S.C. § 1956(a); and (iii) to allow Binance to operate in a manner that would aid and abet pig butchering syndicates that had victimized United States citizens through wire fraud and desired to use the Binance.com exchange as a laundering facility and cash-out point. This association-in-fact enterprise is referred to herein as "Enterprise #1." Binance, BAM, and Zhao participated in and conducted the affairs of Enterprise #1 through a pattern of racketeering activity.

Enterprise #2 (Association-in-Fact Enterprise)

262. Zhao and the individual Binance and BAM employees, officers, and executives

with whom Zhao conspired to violate 18 U.S.C. § 1960(a)—including BAM's then-CEO Brian Shroder and the persons identified in the Binance plea agreement's Statement of Facts as Individuals 1, 2, 3, and 4, all of whom are known to Binance, BAM, and Zhao—constituted an association-in-fact enterprise, the common purposes of which were (i) to allow Binance to operate as an unlicensed money transmitting business, in violation of 18 U.S.C. § 1960(a); (ii) to allow Binance to facilitate and conduct transactions on the Binance.com exchange that the Defendants knew involved illicit proceeds of criminal offenses, in violation of 18 U.S.C. § 1956(a); and (iii) to allow Binance to operate in a manner that would aid and abet pig butchering syndicates that were victimizing United States citizens through wire fraud and desired to use the Binance.com exchange as a laundering facility and cash-out point. This association-in-fact enterprise is referred to herein as Enterprise #2. Zhao directed the conduct of Enterprise #2's affairs through a pattern of racketeering activity.

Enterprise #3 (Binance Corporate Enterprise)

263. Zhao and his Binance employees, officers, and executives conspired to operate Binance (i) as an inherently illegal money transmitting business in violation of 18 U.S.C. § 1960(a), and (ii) in a manner designed to aid, abet, and facilitate pig butchering syndicates' frauds and money laundering. This went on systematically and continuously for years. Binance itself is therefore a corporate RICO enterprise, the conduct for which Zhao can be held responsible as the RICO defendant. The Binance corporate RICO enterprise is referred to herein as Enterprise #3. Defendant Zhao, as then-CEO and mastermind of the Binance corporate RICO enterprise, may be held individually liable for directing that corporate RICO enterprise to operate through a pattern of racketeering activity. In addition, Defendant BAM may be held liable for conspiring with RICO enterprise to violate RICO.

Enterprise #4 (Association-in-Fact Enterprise)

264. Binance, Zhao, and the various pig butchering syndicates that were engaged in ongoing, extensive wire frauds that victimized American citizens and utilized the Binance.com exchange as a laundering facility and cash-out point for illicitly obtained cryptocurrency constituted an association-in-fact RICO enterprise. The common purpose of the enterprise was to use the Binance.com exchange as a laundering facility and a cash-out point for the syndicate(s) ongoing, extensive wire fraud schemes, and thereby to aid, abet, and facilitate the wire frauds and money laundering. In exchange, Binance (and therefore Zhao) received lucrative transaction fees from the pig butchering syndicates. Binance and Zhao participated in the conduct of Enterprise #4's affairs through a pattern of racketeering activity, because they participated in the operation of Enterprise #4's money laundering and cash-out activities that utilized the Binance.com exchange.

Enterprise #5 (Association-in-Fact Enterprise)

265. Each of the criminal syndicates that defrauded the Plaintiffs of millions of dollars constituted a discrete association-in-fact enterprise engaged in an open-ended pattern of racketeering activity (namely, wire fraud and money laundering), the common purpose of which was to steal cryptocurrency from innocent victims (including victims known to be residing in the United States) and then launder those proceeds on centralized cryptocurrency exchanges (including Binance) that were known to be permissive toward such illegal activities. Because it is not presently known whether the Plaintiffs were victimized by a single common syndicate or multiple syndicates (which ultimately is inconsequential to Defendants' RICO liability), these association-in-fact enterprises are referred to herein, collectively, as "Enterprise #5." Binance and Zhao conspired with Enterprise #5 to violate 18 U.S.C. § 1962(c), because they agreed to

facilitate Enterprise #5's wire frauds and money laundering by permitting Enterprise #5 unfettered use of the Binance.com exchange as a laundering facility and essential cash-out point for the otherwise traceable and seizable cryptocurrency assets that Enterprise #5 fraudulently stole from the Plaintiffs (and countless other victims who are not parties to this lawsuit).

B. The RICO Enterprises' Patterns of Racketeering Activity

266. Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 265 above.

Enterprise #1's Racketeering Activity

267. With respect to Enterprise #1, Binance, BAM, and Zhao participated in and/or directed the enterprise's affairs through a pattern of racketeering activity, to wit, operating Binance as an unregistered and unlicensed money transmitting business in violation of 18 U.S.C. § 1960(a) while misleading United States regulators and law enforcement into believing that all U.S.-based customers were being routed to the registered Binance.US exchange. Because the Binance.com exchange operated in violation of 18 U.S.C. § 1960(a), and because a violation of 18 U.S.C. § 1960(a) is a RICO predicate under 18 U.S.C. § 1961(1)(B), every financial transaction that Binance conducted on the Binance.com exchange also was a violation of 18 U.S.C. § 1956(a)(1)(A)(i) by virtue of 18 U.S.C. § 1956(c)(7)(A)'s cross-reference to 18 U.S.C. § 1961(1). Accordingly, Enterprise #1's pattern of racketeering included serial, years-long violations of 18 U.S.C. § 1956, in addition to the serial, years-long violations of 18 U.S.C. § 1960(a).

268. Enterprise #1 and its pattern of racketeering activity began in or around June 2019, when BAM formed Binance.US and registered it with FinCEN to divert United States regulators' and law enforcement's attention away from Binance and ran until at least October

2022. On information and belief, Enterprise #1's pattern of racketeering activity would have continued indefinitely had the United States Department of Justice not conducted its investigation and ultimately its prosecution of Binance and Zhao.

Enterprise #2's and Enterprise #3's Racketeering Activity

269. With respect to Enterprise #2 and Enterprise #3, Zhao was associated with and directed the conduct of each of those enterprises through a pattern of racketeering activity, to wit, (i) operating Binance as an unregistered and unlicensed money transmitting business in violation of 18 U.S.C. § 1960(a), while misleading United States law enforcement into believing that all United States customers were being routed exclusively to the registered and licensed Binance.US exchange, and (ii) aiding and abetting the wire frauds and money laundering, in violation of 18 U.S.C. § 1343 and 18 U.S.C. § 1956(a) respectively, of pig butchering syndicates that Binance and Zhao knowingly permitted to use the Binance.com exchange for criminal purposes.

270. Enterprise #2 and Enterprise #3, and their patterns of racketeering activity, began in or around July 2017, when Zhao launched Binance, and ran until at least October 2022. On information and belief, Enterprise #2's pattern of racketeering activity would have continued indefinitely had the United States Department of Justice not commenced its investigation and ultimately its prosecution of Binance and its Zhao.

Enterprise #4's Racketeering Activity

271. With respect to Enterprise #4, Binance and Zhao were associated with and participated in the conduct of the enterprise's affairs through a pattern of racketeering activity, to wit, (i) aiding and abetting pig butchering syndicates' laundering of the illicit proceeds of the wire frauds on the Binance.com exchange, in violation of 18 U.S.C. § 1956(a), and (ii) thereby aiding and abetting pig butchering syndicates' wire frauds against U.S.-based victims, in

violation of 18 U.S.C. § 1343.

272. Enterprise #4's period of racketeering activity began no later than June 2021 and ended no earlier than November 2022 and involved scores of violations of 18 U.S.C. § 1956(a) and § 1343. On information and belief, Enterprise #4's pattern of racketeering activity would have continued indefinitely, and would have involved more victims and more money laundering on the Binance.com exchange, had the United States Department of Justice not commenced its investigation and ultimately its prosecution of Binance and Zhao for violations of 18 U.S.C. § 1960(a) and the Bank Secrecy Act.

Enterprise #5's Racketeering Activity

273. Enterprise #5 engaged in a pattern of racketeering activity, to wit, (i) using international wire communications to defraud U.S.-based victims, including the Plaintiffs, out of money or property, in violation of 18 U.S.C. § 1343, and (ii) then laundering those illicit proceeds via the Binance.com exchange, in violation of 18 U.S.C. § 1956(a)(1)(A).

274. Enterprise #5's period of racketeering activity began no later than June 2021 and ended no earlier than November 2022 and involved scores of violations of 18 U.S.C. § 1343 and 18 U.S.C. § 1956(a)(1)(A)-(B). By knowingly allowing Binance to be used as a laundering facility and cash-out point for criminal syndicates that were engaged in a variety of international crimes, including wire fraud schemes to defraud Lenny and his co-Plaintiffs, Binance and Zhao conspired with Enterprise #5 to violate 18 U.S.C. § 1962(c) through a pattern of wire frauds and the money laundering that enabled Enterprise #5 to successfully complete those wire frauds.

C. The Causal Connection Between the RICO Enterprises' Racketeering and Plaintiffs' Economic Injuries

275. Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 274 above.

276. Enterprise #1's racketeering activities were a but-for and proximate cause of the Plaintiffs' economic injuries. By enabling Binance to operate as an unlicensed money transmitting business in violation of 18 U.S.C. § 1960(a), Enterprise #1 enabled Binance to circumvent the Bank Secrecy Act's anti-money laundering requirements. As FinCEN concluded from its investigation, Binance's "willful failure to implement an effective [anti-money laundering] program . . . directly led to the [Binance] platform being used to process transactions" designed to "launder illicit proceeds" and "stolen funds." FinCEN also found that Binance's "willful failure to report to FinCEN hundreds of thousands of suspicious transactions inhibited law enforcement's ability to disrupt the illicit actors." Had Binance complied with the applicable anti-money laundering requirements, the pig butchering syndicates that defrauded the Plaintiffs of millions of dollars of USDT would not have been able to launder that USDT on the Binance.com exchange. Instead, Binance would have frozen the syndicates' Binance.com accounts, enabling law enforcement and Tether Ltd. to return the stolen USDT to the Plaintiffs.

277. Enterprise #2's and Enterprise #3's racketeering activities were a but-for and proximate cause of the Plaintiffs' economic injuries. First, Enterprise #2's and Enterprise #3's violations of 18 U.S.C. § 1960(a) enabled the pig butchering syndicates' successful completion of the fraud for the reasons described in the preceding paragraph. Second, because Enterprise #2 and Enterprise #3 aided and abetted the pig butchering syndicates' wire frauds against the Plaintiffs and the syndicates' subsequent laundering of the USDT that they stole from the Plaintiffs, Enterprise #2 and Enterprise #3 (and thus the Defendants who conducted or participated in the affairs of those enterprises through a pattern of racketeering activity) are treated under the law as having committed those wire frauds and money laundering offenses in their own right. Those wire frauds were a but-for and proximate cause of the Plaintiffs'

economic injuries, because those frauds were what caused the Plaintiffs' assets to be stolen in the first place. And the laundering of those stolen assets on the Binance.com exchange was a but-for and proximate cause of the Plaintiffs' economic injuries, because the laundering is what caused the USDT to become unavailable to law enforcement and Tether Ltd., which otherwise would have been able to seize the USDT (or burn and replace it) and thereby to make the Plaintiffs whole.

278. Enterprise #4's racketeering activities were a but-for and proximate cause of the Plaintiffs' economic injuries. Enterprise #4's racketeering activities included (i) the underlying wire frauds that victimized the Plaintiffs, and (ii) the money laundering on the Binance.com exchange that made the Plaintiffs' economic losses permanent, for the reasons explained above. Those racketeering acts were a but-for and proximate cause of the Plaintiffs' economic injuries, because the wire frauds were what caused the Plaintiffs' assets to be stolen in the first place and the laundering of those stolen assets on the Binance.com exchange is what caused the USDT to become unavailable to law enforcement and Tether Ltd. By aiding and abetting those wire frauds and money laundering activities, Binance and Zhao are treated under the law as having committed those wire frauds and money laundering activities in their own right.

279. Enterprise #5's racketeering activities were a but-for and proximate cause of the Plaintiffs' economic injuries. Enterprise #5's racketeering activities included (i) the underlying wire frauds that victimized the Plaintiffs, and (ii) the money laundering on the Binance.com exchange that made the Plaintiffs' economic losses permanent, for the reasons explained above. Those racketeering acts were a but-for and proximate cause of the Plaintiffs' economic injuries, because the wire frauds were what caused the Plaintiffs' assets to be stolen in the first place and the laundering of those stolen assets on the Binance.com exchange is what caused the USDT to

become unavailable to law enforcement and Tether Ltd. By conspiring with Enterprise #5 to facilitate Enterprise #5's wire frauds and money laundering activities (*i.e.*, conspiring with Enterprise #5 to violate RICO), Binance and Zhao are liable for the economic injuries that Enterprise #5's caused the Plaintiffs, and Binance's and Zhao's conspiratorial conduct enabled Enterprise #5 to succeed.

COUNT ONE

(Defendants Binance, BAM, and Zhao)

(18 U.S.C. § 1964(c), for violations of 18 U.S.C. § 1962(c))

280. The Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 279 above.

281. Binance, BAM, and Zhao were each associated with Enterprise #1 and participated in and/or directed the conduct of Enterprise #1's affairs through a pattern of racketeering activity as described above.

282. Enterprise #1's racketeering activities, as directed and conducted by Binance, BAM, and Zhao, were a but-for and proximate cause of the Plaintiffs' economic injuries for the reasons described above.

COUNT TWO

(Defendant Zhao)

(18 U.S.C. § 1964(c), for violations of 18 § U.S.C. 1962(c))

283. The Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 279 above.

284. Zhao was associated with Enterprise #2 and directed the conduct of Enterprise #2's affairs through a pattern of racketeering activity as described above, including by directing

Enterprise #2 to aid and abet the wire frauds and money laundering of pig butchering syndicates that Zhao knew were using the Binance.com exchange for criminal purposes.[6]

285. Enterprise #2's racketeering activities, as directed and conducted by Zhao, were a but-for and proximate cause of the Plaintiffs' economic injuries for the reasons described above.

COUNT THREE

(Defendant Zhao)

(18 U.S.C. § 1964(c), for violations of 18 U.S.C. § 1962(c))

286. The Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 279 above.

287. Zhao was associated with Enterprise #3 and directed the conduct of Enterprise #3's affairs through a pattern of racketeering activity as described above, including by directing Enterprise #3 (*i.e.*, Binance) to aid and abet the wire frauds and money laundering of the pig butchering syndicates that Zhao knew were using the Binance.com exchange for criminal purposes.

288. Enterprise #3's racketeering activities, as directed and conducted by Zhao, were a but-for and proximate cause of the Plaintiffs' economic injuries for the reasons described above.

[6] To be clear, this complaint is not alleging that Zhao aided and abetted another's violation of RICO. The complaint is alleging that, at the direction of Zhao, the RICO enterprise whose affairs Zhao directed engaged in conduct that constituted aiding and abetting of the RICO predicate acts of wire fraud and money laundering, which means the RICO enterprise itself committed the predicate acts of wire fraud and money laundering. *See, e.g.*, *Jaguar Cars v. Royal Oaks Motor Car Co.*, 46 F.3d 258, 270 (3d Cir. 1995). The same is true of the other causes of action that are based in part on an aiding and abetting theory; *Trustees of Boston Univ. v. ASM Communs., Inc.*, 33 F. Supp. 2d 66, 72 n.6 (D. Mass. 1998) ("The First Circuit has held that predicate acts under RICO can include aiding and abetting mail or wire fraud." (citing *Aetna Cas. Su. Co. v. P&B Autobody*, 43 F.3d 1546, 1560 (1st Cir. 1994))).

COUNT FOUR

(Defendants Binance and Zhao)

(18 U.S.C. § 1964(c), for violations of 18 U.S.C. § 1962(c))

289. The Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 279 above.

290. Binance and Zhao were each associated with Enterprise #4 and participated in the conduct of Enterprise #4's affairs through a pattern of racketeering activity as described above, including by aiding and abetting the wire frauds and money laundering of the pig butchering syndicates that Zhao and Binance knew were using the Binance.com exchange for criminal purposes.

291. Enterprise #4's racketeering activities, as directed and conducted by Zhao and Binance, were a but-for and proximate cause of the Plaintiffs' economic injuries for the reasons described above.

COUNT FIVE

(Defendant BAM)

(18 U.S.C. § 1964(c), for violations of 18 U.S.C. § 1962(d))

292. The Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 279 above.

293. BAM conspired with Enterprise #3 and its pattern of racketeering activity—*i.e.*, conspired with Enterprise #3 to violate 18 U.S.C. § 1962(c)—as described above.

294. Enterprise #3's racketeering activities were a but-for and proximate cause of the Plaintiffs' economic injuries for the reasons described above.

295. Because it conspired with Enterprise #3 and its racketeering activities—*i.e.*,

conspired with Enterprise #3 to violate 18 U.S.C. § 1962(c)—BAM is liable for the economic injuries that Enterprise #3's racketeering activities caused the Plaintiffs.

COUNT SIX

(Defendants Binance and Zhao)

(18 U.S.C. § 1964(c), for violations of 18 U.S.C. § 1962(d))

296. The Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 279 above.

297. Binance and Zhao conspired with Enterprise #5 and its pattern of racketeering activity—*i.e.*, conspired with Enterprise #5 to violate 18 U.S.C. § 1962(c)—as described above.

298. Enterprise #5's racketeering activities were a but-for and proximate cause of the Plaintiffs' economic injuries for the reasons described above.

299. Because they conspired with Enterprise #5 and its racketeering activities—*i.e.*, conspired with Enterprise #5 to violate 18 U.S.C. § 1962(c)—Biance and Zhao are liable for the economic injuries that Enterprise #5's racketeering activities caused the Plaintiffs.

PRAYER FOR RELIEF

WHEREFORE, each and every Plaintiff prays for the following relief:

1. An order holding that the Defendants are jointly and severally liable for the financial injuries the Plaintiff suffered as a result of either the racketeering acts that the Defendants committed or aided and abetted, or the RICO violations that the Defendants conspired to commit;

2. An order trebling the damages for which the Defendants are liable;

3. An award of statutory attorney's fees and costs; and

4. Any other relief that the court deems just and proper.

Respectfully submitted,

Dated: February 26, 2025

/s/ Aaron M. Katz

Aaron M. Katz
Keira Zirngibl
Patrick Dolan
AARON KATZ LAW LLC
399 Boylston Street, 6th Floor
Boston, MA 02116
(617) 915-6305
akatz@aaronkatzlaw.com
kzirngibl@aaronkatzlaw.com
pdolan@aaronkatzlaw.com

Eric Rosen
Constantine P. Economides
(admitted *pro hac vice*)
Lance Aduba (*pro hac vice*
forthcoming)
DYNAMIS LLP
225 Franklin Street, 26th Floor
Boston, MA 02110
(617) 802-9157
erosen@dynamisllp.com
ceconomides@dynamisllp.com
laduba@dynamisllp.com

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing was served on counsel of record for all parties via the CM/ECF system on February 26, 2025.

/s/ Aaron M. Katz